

WILL THE CAN-SPAM ACT OF 2003 FINALLY PUT A LID ON UNSOLICITED E-MAIL?

INTRODUCTION

In 1985, only 2000 computers were connected to the Internet.¹ Today, more than 100 million American adults use e-mail every day.² E-mail has been described as the “killer app” of the Internet era because it has revolutionized the way in which people communicate with business associates, family, and friends.³ In the past decade, however, a dramatic increase in unsolicited commercial e-mail, or “spam,” is threatening to “kill the ‘killer app....’”⁴ Spam accounts for as much as eighty percent⁵ of the estimated fifty-seven billion e-mail messages that are transmitted across the Internet daily.⁶ Because of the financial and technological burdens it imposes, as well as its associations with fraud, pornography, and computer viruses, spam presents real threats to American business, children, and the elderly, and jeopardizes the very future of the Internet. The CAN-SPAM Act of 2003 (CAN-SPAM)⁷ was enacted in an attempt to stem these harmful effects.

Many people involved in the anti-spam struggle believe that the law is

-
1. JANET ABBATE, *INVENTING THE INTERNET* 186 (1999).
 2. DEBORAH FALLOWS, PEW INTERNET & AMERICAN LIFE PROJECT, *SPAM: HOW IT IS HURTING EMAIL AND DEGRADING LIFE ON THE INTERNET* 6 (Oct. 22, 2003), available at http://www.pewinternet.org/pdfs/PIP_Spam_Report.pdf.
 3. *Id.*
 4. *Spam (Unsolicited Commercial E-Mail): Hearing on S.R.253 Before Senate Comm. on Commerce, Sci. & Transp.*, 108th Cong. (May 21, 2003) (testimony of Orson Swindle, Commissioner, Federal Trade Commission), available at http://commerce.senate.gov/hearings/testimony.cfm?id=773&wit_id=2088.
 5. Tricia Bishop, *Turning Up the Heat on Spam*, BALT. SUN, Nov. 28, 2004, at 1C; David McGuire, *A Year After Legislation, Spam Still Widespread*, WASH. POST, Jan. 4, 2005, at E5.
 6. Hiawatha Bray, *As War on Spam Heats Up, Many Valid E-Mails Are Getting Lost*, BOSTON GLOBE, Feb. 18, 2004, at A14.
 7. 15 U.S.C.A. §§ 7701-7713 (West Supp. 2004).

powerless to stop spam.⁸ Anti-spam statutes enacted in more than two-thirds of the states since 1997 have been unable to reduce the flow of unwanted advertisements into users' e-mail in-boxes.⁹ Critics of the CAN-SPAM Act believe that a federal law will be no more effective than the state laws were.¹⁰ It is true that no law will be a "silver bullet" capable of eliminating spam by itself.¹¹ Legislation does, however, have an important role to play in eradicating spam. CAN-SPAM imposes criminal liability on the worst e-mail abuses, and sets up a uniform nationwide framework of regulations for most commercial e-mail.¹² When combined with industry cooperation, consumer education, and most importantly, technological developments, these provisions will make progress toward significantly reducing spam, and ensuring that e-mail will continue to develop as a dependable means of personal and business communication.¹³

This Note begins by discussing the origins and implications of the spam problem in Part I. This Note continues in Part II with an analysis of the CAN-SPAM Act of 2003, including a description of the common provisions of state laws that preceded the federal statute, and an explanation of what the CAN-SPAM Act does—and does not do—to regulate spam. Finally, in Part III, this Note will suggest that the spam problem can be solved only by the combination of legislation and technological developments.

I. THE PROBLEM

This section will sketch the history of spam from a single message posted to a handful of newsgroups ten years ago¹⁴ to a ten billion dollar problem bearing down on the Internet today.¹⁵ The risks presented by spam, specifically its economic impact, its threat to the elderly and to children, and its potential to crush the infrastructure of the Information Superhighway¹⁶ will be identified. Finally, this section will describe some of the steps that computer scientists, businesspeople, and individuals have

8. See Matthew Prince, Address at the 2004 Spam Conference at the Massachusetts Institute of Technology (Jan. 16, 2004) (transcript on file with the author), available at <http://spamconference.org/webcast.html> (webcast only available on-line).

9. See *infra* Part II.A.

10. See *infra* Part III.A.

11. 149 CONG. REC. S15,944 (daily ed. Nov. 25, 2003) (statement of Sen. Wyden).

12. See *infra* Part II.B.

13. 149 CONG. REC. H12,860 (daily ed. Dec. 8, 2003) (statement of Rep. Sensenbrenner).

14. LAURENCE A. CANTER & MARTHA S. SIEGEL, HOW TO MAKE A FORTUNE ON THE INFORMATION SUPERHIGHWAY 21 (1994).

15. Neil Swidey, *SpamBusters*, BOSTON GLOBE, Oct. 5, 2003 (Magazine), at 12, 14.

16. See generally ALAN SCHWARTZ & SIMSON GARFINKEL, STOPPING SPAM 1-11 (1998).

taken to defend themselves from the onslaught of spam.¹⁷

A. What is Spam?

In general, spam¹⁸ refers to any unwanted e-mail.¹⁹ More precise definitions of spam vary.²⁰ In fact, one of the initial difficulties in dealing with the spam problem is the lack of consensus as to what spam actually is.²¹ A broader definition of spam includes *all* unsolicited bulk e-mail (UBE), regardless of the source or content.²² A narrower view includes only unsolicited bulk commercial e-mail (UCE).²³ To most computer users,

17. *Id.* at 66.

18. SPAM is a canned processed meat product manufactured by Hormel Foods Corp. *Id.* at 11. According to Hormel, the use of the term “spam” to describe unsolicited commercial e-mail is in reference to a skit on the British sketch comedy show *Monty Python’s Flying Circus*. *Id.*; HORMEL FOODS CORP., *SPAM and the Internet*, at http://www.spam.com/ci/ci_in.htm (last visited Feb. 19, 2005). “In this skit, a group of Vikings sang a chorus of ‘spam, spam, spam. . .’ in an increasing crescendo, drowning out other conversation. Hence, the analogy applied because [unsolicited commercial e-mail] was drowning out normal discourse on the Internet.” *Id.* The term “spam” was first used in an Internet context by players in interactive adventure games called multi-user dungeons (MUDs). SCHWARTZ & GARFINKEL, *supra* note 16, at 11. When certain players repeatedly posted the same message in the chat room, the other players scolded the offender for filling the screen with “spam.” *Id.* For the most part, Hormel has come to terms with the use of “spam” as the generic term for unsolicited e-mail. *See* HORMEL FOODS CORP., *supra*. Hormel, however, continues to defend its brand name fiercely against what it sees as improper commercial use of the word. *See, e.g.*, Hormel Foods Corp. v. Jim Henson Prods., 73 F.3d 497 (2d Cir. 1996) (claiming copyright and trademark violations when a puppet named “Spa’am” was featured in a children’s movie).

19. SCHWARTZ & GARFINKEL, *supra* note 16, at 1 (describing spam as “the Internet’s version of junk mail, telemarketing calls during dinner, crank phone calls, and leaflets pasted around town, all rolled up into a single annoying electronic bundle”). In contrast to the derogatory term “spam” used to describe unwanted e-mail, desirable messages are sometimes called “ham.” Swidey, *supra* note 15, at 14.

20. David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. REV. 325, 327 (2001).

21. *See* PETER A. JOHNSON, DIRECT MARKETING ASSOCIATION, WHAT COMMERCIAL E-MAIL CONTRIBUTES TO THE U.S. ECONOMY 4 (May 20, 2003) (on file with the author). An unsolicited e-mail message that may be an unwelcome annoyance to one computer user may be an unexpected retail opportunity to another. *Id.* Some have described spam in the same way Justice Potter Stewart defined obscenity—“[we] know it when [we] see it.” Swidey, *supra* note 15, at 26; Joseph P. Kendrick, “Subject: ADV:” *Anti-Spam Laws Force Emerging Internet Business Advertisers to Wear the Scarlet “S,”* 7 J. SMALL & EMERGING BUS. L. 563, 566 & 566 n.7 (2003) (quoting *Jacobellis v. Ohio*, 378 U.S. 184, 197 (1964) (Stewart, J., concurring)).

22. Sorkin, *supra* note 20, at 327.

23. *Id.* at 328.

the distinction is irrelevant—they just want the spam to stop coming.²⁴ However, the taxonomy of spam takes on some importance in fashioning technical and legal remedies to the problem.²⁵ Because the CAN-SPAM Act of 2003 regulates only unsolicited commercial e-mail,²⁶ this Note will limit its discussion to the efforts to control UCE.

B. Where Did Spam Come From?

E-mail began in 1969, when the Advanced Research Project Agency (ARPA) set up ARPANET, a network of computer systems maintained by the military, defense contractors, and universities.²⁷ ARPANET was created to facilitate scientific and military research throughout the country by providing a means for quick and secure electronic communications.²⁸ Over time, ARPANET fell into disuse, and other networks developed by academics and businesses were established.²⁹ These networks were linked to the remnants of ARPANET, and thus, the Internet was created.³⁰

Until the mid-1990s, only a very small number of people—nearly all of them scientists and military personnel—used the Internet.³¹ However, computer ownership and Internet usage among the general public has exploded in recent years.³² Today, the Internet, and e-mail specifically, is a part of daily life for a majority of Americans.³³ In fact, approximately six

-
24. UNSPAM, *Spam Numbers & Statistics*, at http://www.unspam.com/fight_spam/information/spamstats.html?start=40 (last visited Apr. 14, 2005) (noting that seventy-three percent of voters strongly support banning unsolicited e-mail).
 25. Sorkin, *supra* note 20, at 334. For example, governmental regulation of unsolicited political and religious messages implicates prickly First Amendment issues that are avoided if the action is limited to commercial messages. *Id.*
 26. *See generally* CAN-SPAM Act of 2003, 15 U.S.C.A. §§ 7701-7713 (West Supp. 2004).
 27. ABBATE, *supra* note 1, at 64; *see also* ACLU v. Reno, 929 F. Supp. 824, 830-49 (E.D. Pa. 1996). The ACLU court's findings of fact include a detailed history of the Internet and an exhaustive explanation of its inner workings. *Id.*
 28. ABBATE, *supra* note 1, at 43-81.
 29. *Id.* at 96-99.
 30. *Id.* at 113.
 31. *See id.* at 84.
 32. *See* U.S. CENSUS BUREAU, U.S. DEP'T OF COMMERCE, HOME COMPUTERS AND INTERNET USE IN THE UNITED STATES: AUGUST 2000, at 2 (Sept. 2001), available at <http://www.census.gov/prod/2001pubs/p23-207.pdf>. The Census Bureau began tracking Internet use in 1997. *Id.* At that time, only eighteen percent of American households had Internet access. *Id.* By 2000, that number had jumped to forty-two percent. *Id.*
 33. JOHNSON, *supra* note 21, at 4 (noting that approximately sixty-one percent of American adults—nearly 130 million people—use e-mail daily).

trillion e-mail messages are now sent annually.³⁴ Such widespread use has placed e-mail alongside other means of communication—telephones, fax machines, and the U.S. Postal Service—upon which Americans depend.³⁵ This huge number of daily e-mail users presents an irresistible opportunity for marketers to pitch their products on-line.³⁶

Advertisements were rare on the Internet in its early days.³⁷ That all changed on April 12, 1994, when spam was born.³⁸ On that day, Laurence Canter and his wife Martha Siegel—lawyers, no less—figured out a way to “blast” an ad for immigration law services to about 6000 newsgroups on Usenet.³⁹ The message enraged many subscribers who bristled at commercial use of the Internet.⁴⁰ Despite the outrage, the message was a success.⁴¹ The posting, which cost Canter and Siegel practically nothing, generated nearly \$100,000 in revenue.⁴² Soon, other marketers realized the potential of e-mail as a cheap and efficient means of contacting potential customers.⁴³ The combination of an ever-growing audience, and the cost-

-
34. 149 CONG. REC. H12,192 (daily ed. Nov. 21, 2003) (statement of Rep. Sensenbrenner).
 35. JOHNSON, *supra* note 21, at 5.
 36. See CANTER & SIEGEL, *supra* note 14, at 13.
 37. See *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1018 (S.D. Ohio 1997).
 38. Swidey, *supra* note 15, at 14. Although spam did not debut until 1994, its coming was foretold by a few farsighted Internet pioneers. As early as 1975, programmer Jon Postel identified a “fundamental flaw” in ARPA: There was no means of selectively refusing messages; in order to view *any* messages, a user had to view *all* messages received. SCHWARTZ & GARFINKEL, *supra* note 16, at 17-18. In 1993, Paul Vixie, a prominent computer programmer, publicly scolded a Penn State University sociology professor for mass-mailing a survey. “[T]he effect of your survey is to hasten the Internet’s downslide into common-market status. We must establish, here and every day thereafter, that unsolicited mass mailings are strongly prohibited....” *Id.* at 21-22. These warnings went unheeded, however, and spam has enjoyed nearly unrestricted growth.
 39. See CANTER & SIEGEL, *supra* note 14, at 21. Canter and Siegel “pushed a single key ... [and] ... sent [their] message to millions of people in every corner of the world.” *Id.*
 40. Swidey, *supra* note 15, at 14. The Internet of the early 1990s has been described as a “techie country club, open mainly to academics and computer engineers,” who frowned on “crass commercialism.” *Id.* at 12; see also CANTER & SIEGEL, *supra* note 14, at 21-24. Canter and Siegel were bombarded with “flames” (caustic e-mail messages), e-mail bombs (huge computer files sent to jam the recipient’s system), and even death threats. *Id.*
 41. Swidey, *supra* note 15, at 14.
 42. CANTER & SIEGEL, *supra* note 14, at 2; Swidey, *supra* note 15, at 14.
 43. *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1018 (S.D. Ohio 1997). The court in *CompuServe* observed that “there is no per-message charge to

savings of e-mail advertising made commercial e-mail a bonanza for marketers.⁴⁴ Within a few years, established businesses with good reputations began to use bulk e-mail as a means of communicating with customers.⁴⁵

Consumers spend a significant amount of money on-line today.⁴⁶ Consequently, on-line marketers see huge revenue potential in e-mail advertising.⁴⁷ If no one were buying, the spammers would stop sending messages.⁴⁸ But people are buying, and in huge numbers.⁴⁹ One study indicates that more than one-third of e-mail users have made a purchase in response to some kind of e-mail message.⁵⁰ Significantly, more than ten million Americans report that they have made a purchase in response to an *unsolicited* e-mail message.⁵¹ Today, spam accounts for as much as eighty percent of all e-mail messages sent.⁵² The amount of spam in Americans' in-boxes has increased dramatically in a short time.⁵³ This precipitous rise in spam volume has mobilized programmers, businesspeople, and individuals to take action.⁵⁴

C. Why Fight Spam?

The risks posed by spam are real, and they require immediate action.⁵⁵

send electronic messages over the Internet and such messages usually reach their destination within minutes." *Id.*

44. CANTER & SIEGEL, *supra* note 14, at 215-16.

45. SCHWARTZ & GARFINKEL, *supra* note 16, at 3 (noting that by 1998, companies like AT&T and Amazon.com had begun to use bulk e-mail); *see also* Saul Hansell, *It Isn't Just the Peddlers of Pills: Big Companies Add to Spam Flow*, N.Y. TIMES, Oct. 28, 2003, at A1.

46. JOHNSON, *supra* note 21, at 5 (estimating that at least \$1.5 billion is spent on purchases in response to unsolicited e-mail messages).

47. CANTER & SIEGEL, *supra* note 14, at 215-16.

48. Brian McWilliams, *Swollen Orders Show Spam's Allure*, WIRED NEWS, Aug. 6, 2003, at <http://www.wired.com/news/business/0,1367,59907,00.html>.

49. JOHNSON, *supra* note 21, at 4-5.

50. *Id.* at 4.

51. *Id.* at 1. A New Hampshire direct marketer inadvertently posted its order logs on the Internet, revealing that, in a four-week period, more than 6000 people paid fifty dollars each for penis enlargement pills advertised in an e-mail message. McWilliams, *supra* note 48.

52. Bishop, *supra* note 5.

53. *See* SCHWARTZ & GARFINKEL, *supra* note 16, at 4 (noting that in 1997, only five to fifteen percent of e-mail was spam).

54. 149 CONG. REC. S13,025 (daily ed. Oct. 22, 2003) (statement of Sen. Schumer) (observing that we are "under siege" by "[a]rmies of online marketers").

55. *Id.*

The problems with spam are many, and range from a minor annoyance to a real threat to the integrity of the hardware and networks that make up the Internet.⁵⁶ Spam wastes time and money and erodes people's confidence in e-mail as an effective communication tool.⁵⁷ Also, spam's association with fraud and pornography poses a risk to the elderly, children, and anyone lacking the Internet savvy to avoid falling prey to e-mail scams.⁵⁸

1. Cost

Spam is cheap to send, but it carries high costs for the recipients.⁵⁹ The cost of spam can be measured in time, dollars, and bandwidth.⁶⁰ Spam is estimated to cost Americans \$10 billion each year,⁶¹ and that cost is expected to increase dramatically if nothing is done to turn the tide.⁶² What makes these costs especially objectionable is that they are borne, in great part, by the recipients and not the senders of spam.⁶³

The most significant difference between spam and other forms of advertising is the cost to the advertiser.⁶⁴ A full-page advertisement in a major newspaper can cost \$25,000, and a catalog mailing to 100,000 homes can cost \$150,000, but a spammer can send 10,000 e-mail messages for around a penny.⁶⁵ While cost concerns encourage traditional marketers to target their advertising efforts to maximize the return on their investment, spammers have no motivation to target their message due to the negligible cost of e-mail advertising.⁶⁶ The greatest part of the cost of transmitting spam is borne by the recipient.⁶⁷ Spammers make use of the recipient's

56. Bill Gates, *Why I Hate Spam*, WALL ST. J., June 23, 2003, at A14.

57. FALLOWS, *supra* note 2, at 7.

58. Gates, *supra* note 56.

59. Media3 Technologies, L.L.C. v. Mail Abuse Prevention System, L.L.C., No. 00-CV-12524-MEL, 2001 U.S. Dist. LEXIS 1310, at *2 (D. Mass. Jan. 2, 2001); *see also* SCHWARTZ & GARFINKEL, *supra* note 16, at 5-6.

60. *See* SCHWARTZ & GARFINKEL, *supra* note 16, 6-11.

61. Swidey, *supra* note 15, at 14. The annual worldwide cost of spam is estimated at \$25 billion. BRIAN MCWILLIAMS, SPAM KINGS 295 (2005).

62. UNSPAM, *supra* note 24, at 36 (estimating that by 2007, spam's cost in lost productivity will approach \$75 billion).

63. Sorkin, *supra* note 20, at 337-38.

64. SCHWARTZ & GARFINKEL, *supra* note 16, at 5.

65. *Id.*; *see also* Jack Hitt, *Confessions of a Spam King*, N.Y. TIMES, Sept. 28, 2003 (Magazine), at 48, 50 (indicating that a spammer can send one million messages for as little as \$25).

66. SCHWARTZ & GARFINKEL, *supra* note 16, at 5; *see also* MCWILLIAMS, *supra* note 61, at 173 (noting that a "good response rate" of 0.2%—just 100 sales from 50,000 messages—represents thousands of dollars in revenue for a spammer).

67. This is particularly true for Internet users who must incur per-minute access charges,

Internet connection and computer equipment to get the message to its destination. This is comparable to a telemarketer calling your home collect, or a retailer mailing a catalog to your home postage due.⁶⁸

Spam wastes time, and time is money.⁶⁹ Companies experience lost productivity when IT staff spend time updating software filters to block spam, and when rank-and-file employees take time to manually delete the messages that get through software filters.⁷⁰ Over time, this loss of productivity has an effect on the company's bottom line.⁷¹

Internet Service Providers (ISPs) must spend money on additional hardware to increase server capacity to handle the greater demands imposed by spam.⁷² "High volumes of junk e-mail devour computer processing and storage capacity, [and] slow down data transfer between computers over the Internet by congesting the electronic paths through which the messages travel...."⁷³ The increased hardware costs to ISPs due to spam volume are likely to be passed on to consumers, making access to the Internet more expensive.

2. Spam Reduces People's Reliance on E-mail

It is clear that Internet users are annoyed by spam.⁷⁴ However, mere

or subscribers who access the Internet via a dial-up connection to a telephone number outside their local calling area. *See* 149 CONG. REC. S15,947 (daily ed. Nov. 25, 2003) (statement of Sen. Burns). In rural areas, many consumers are unable to access the Internet without incurring long-distance telephone charges. The more time such an e-mail user spends on-line sorting through spam, the more long-distance charges he will incur. *See id.*

68. *See* *Ferguson v. Friendfinders, Inc.*, 115 Cal. Rptr. 2d 258, 268 (Ct. App. 1 Dist. 2002). Another analogy to the cost-shifting effect of spam is unsolicited commercial faxes. *See* *Aronson v. Bright-Teeth Now, L.L.C.*, 57 Pa. D. & C. 4th 1, *4-5 (Pa. Com. Pl. June 19, 2002), *aff'd*, 824 A.2d 320 (Pa. Super. Ct. 2003). Because the recipient bears the cost of paper, ink, and temporary loss of use of their fax machine, the Telephone Consumer Protection Act of 1991 prohibits sending unsolicited advertisements to fax machines. 47 U.S.C. § 227(b)(1)(C) (2000).

69. *See* *Intel Corp. v. Hamidi*, 71 P.3d 296, 328 (Cal. 2003) (Mosk, J., dissenting).

70. *See id.*; *see also* UNSPAM, *supra* note 24 (noting that more than half of the companies in one survey reported that a top IT priority is the reduction of spam).

71. *See Intel Corp.*, 71 P.3d at 328.

72. This problem became immediately apparent when spam debuted. After they sent the very first spam message in 1994, Laurence Canter and Martha Seigel's ISP's server crashed because it was unable to handle the increased traffic generated by the message. *See* SCHWARTZ & GARFINKEL, *supra* note 16, at 22.

73. *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1028 (S.D. Ohio 1997).

74. *See* UNSPAM, *supra* note 24 (noting that ninety-six percent of e-mail users find spam "annoying").

annoyance is not enough to justify an all-out war on spam.⁷⁵ Or is it? Spam endangers “the viability of electronic mail as an effective means of communication.”⁷⁶ Senator Charles Schumer, testifying before a senate committee in support of his “Do-Not-Spam” Registry legislation,⁷⁷ said “[i]f spam continues to grow, people will rely on their email less and less.”⁷⁸ E-mail has been hailed as the “killer app” of the Internet age because of its potential to revolutionize personal and business communication.⁷⁹ There are indications, however, that some computer users have become so frustrated by spam that they have chosen to terminate their Internet access accounts, and forgo e-mail altogether.⁸⁰ Businesses are beginning to wonder whether e-mail really is a productivity-boosting communications tool, or a drain on resources.⁸¹ Senator Schumer identified decreased reliance on e-mail as a major risk of spam, and urged his fellow legislators to act because, “spammers must not be allowed to bog down the vast potential of ... the Internet.”⁸²

-
75. See *U-Haul, Inc. v. WhenU.com, Inc.*, 279 F. Supp. 2d 723, 725 (E.D. Va. 2003) (calling spam the “ugly brother” of pop-up ads, but opining that “[a]las, we computer users must endure [them] as a burden of using the Internet”).
76. *CompuServe Inc.*, 962 F. Supp. at 1028.
77. See *infra* text accompanying notes 206-28.
78. *Spam (Unsolicited Commercial E-Mail): Hearing on SR-253 Before Senate Comm. on Commerce, Sci. & Transp.*, 108th Cong. (2003) (testimony of Charles Schumer) [hereinafter *Schumer Testimony*], available at http://commerce.senate.gov/hearings/testimony.cfm?id=773&wit_id=2087.
79. See FALLOWS, *supra* note 2, at 6.
80. See *CompuServe Inc.*, 962 F. Supp. at 1023 (noting that in one month in 1996, CompuServe received 9970 complaints from subscribers about spam. CompuServe claimed that “[m]any subscribers ... terminated their accounts specifically because of the unwanted receipt of bulk e-mail messages”).
81. See Grant Gross, *Do Antispam Laws Have a Dark Side?*, PC WORLD, Oct. 30, 2003, available at <http://www.peworld.com/news/article/0,aid,113200,00.asp>. “If the problem continues to grow at the rate it currently is growing, it will be impossible for businesses to rely on the Internet and e-mail as a form of communication.” *Id.*; see also Mary Anne Ostrom, *Biggest Law Firm in California Sues Over Spam*, SAN JOSE MERCURY NEWS (Cal.), Mar. 15, 2002, at 3C.
82. *Schumer Testimony*, *supra* note 78; see also SCHWARTZ & GARFINKEL, *supra* note 16, at 10. Some have predicted that e-mail could follow the same path as CB radio, which was designed as a means of two-way communication, but fell into disuse after abusers used the airwaves to broadcast music, advertisements, and political messages. See *id.* at 10-11. But see DEBORAH FALLOWS, PEW INTERNET & AMERICAN LIFE PROJECT, *CAN-SPAM A YEAR LATER* 3-4 (Apr. 2005), available at http://www.pewinternet.org/pdfs/PIP_Spam_Ap05.pdf. A survey conducted one year after CAN-SPAM took effect suggests that spam’s negative effects on people’s e-mail usage is diminishing. In January 2005, fifty-three percent of survey respondents reported that “spam has made them less trusting of email in general,” compared to

Even if spam does not kill e-mail as a communication tool, it does limit the potential of legitimate e-mail marketing as an area for economic growth.⁸³ The Direct Marketing Association (DMA), a trade group promoting catalog, direct mail, and Internet retailing, points to unscrupulous spammers who use fraudulent tactics as “the scourge of consumers and marketers alike.”⁸⁴ According to the DMA, “the American consumer and the direct and interactive marketing industry share a common goal: stamping out the fraud that is cluttering our in-boxes and draining our pocketbooks while, at the same time, growing the legitimate e-mail marketplace.”⁸⁵

3. Fraud

Because spam can be sent cheaply and with relative anonymity, it is the perfect tool for con artists. E-mail scams put the Internet’s most vulnerable users, particularly the elderly, at risk.⁸⁶ When spammers use misleading “from” and “subject” headers, even savvy e-mail users are at risk.⁸⁷ The pervasiveness of fraud in spam makes all commercial e-mail suspect,⁸⁸ thereby limiting the economic potential of e-mail as a selling tool.⁸⁹

4. Pornography

One of the biggest concerns of anti-spam activists is protecting the Internet’s youngest users from exposure to pornographic images in spam messages.⁹⁰ Spammers advertising on-line pornography Web sites often include images in the messages depicting nudity and graphic sex acts.⁹¹ The

sixty-two percent in February 2004. *Id.*

83. See JOHNSON, *supra* note 21, at 7-8.

84. *Id.* at 8.

85. *Id.*

86. See Don Oldenburg, *You’ve Got Deceit: E-Mail Scams Grow*, WASH. POST, Sept. 30, 2003, at C9.

87. *See id.*

88. See Katie Dean, *Survey Confirms It: Spam Sucks*, WIRED NEWS, Oct. 23, 2003, at <http://www.wired.com/news/culture/0,1284,60935,00.html> (“There’s this sense of deception, that is new and different and changing the whole aura of e-mail.... People are approaching their e-mail with a sense of dread.”).

89. See JOHNSON, *supra* note 21, at 8.

90. See FED. TRADE COMM’N, FALSE CLAIMS IN SPAM 12 (Apr. 30, 2003), available at <http://www.ftc.gov/reports/spam/030429spamreport.pdf>; see also Schumer Testimony, *supra* note 78. Senator Schumer expressed frustration that he was “virtually powerless to prevent [pornographic spam] from reaching my daughter’s inbox.” *Id.*

91. See FED. TRADE COMM’N, *supra* note 90, at 13 (noting that seventeen percent of

2005]

CAN-SPAM ACT OF 2003

971

risk that children will see these images is heightened by the practice of using misleading “from” and “subject” headers on spam messages, making it more likely that a young e-mail user will inadvertently open a pornographic message.⁹²

Pornographic spam may also pose a problem in the workplace.⁹³ For a long time, spam has primarily affected personal e-mail accounts,⁹⁴ but recently, there has been a sharp increase in the amount of spam, particularly pornographic spam, received at work.⁹⁵ Surveys have shown that employees feel that pornographic spam received at work can contribute to a hostile work environment, making employers vulnerable to sexual harassment lawsuits.⁹⁶

D. A Losing Battle?

Until recently, the war against spam has been waged by businesspeople, computer programmers, and individual computer users battling on the front lines without the aid of courts and legislatures.⁹⁷ The self-help undertaken by computer users includes manual filtering, software filtering, and private “no-spam” registry services.⁹⁸ Some users have even resorted to retaliating against spammers with vigilante tactics like e-mail bombs, denial-of-service attacks, and “black holing.”⁹⁹

1. Manual Filtering

Manual filtering is the simplest, though far from most efficient, means

pornographic spam messages contain “adult” images).

92. *See id.* (noting that forty-one percent of pornographic spam messages containing adult images have false statements in their “from” or “subject” headers).

93. *See* Tim Lemke, *Lawyers Detect Gold in the E-Mail; Employers Left Vulnerable to Harassment Lawsuits*, WASH. TIMES, Oct. 16, 2003, at A1.

94. *See* FALLOWS, *supra* note 2, at 18.

95. Lemke, *supra* note 93.

96. *See id.* (noting that sixty-two percent of employees felt that pornographic e-mail can contribute to a hostile work environment, and that sixty-four percent of employees felt that employers had a duty to shield employees from unwanted pornographic e-mail).

97. *See, e.g., Intel Corp. v. Hamidi*, 71 P.3d 296, 301 (Cal. 2003) (noting that before suing the defendant spammer, Intel demanded that the spammer stop sending the unwanted messages, and also attempted to use technology to block delivery); *see also CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1017 (S.D. Ohio 1997) (describing similar steps taken by CompuServe prior to bringing suit against a spammer).

98. *See infra* text accompanying notes 100-24.

99. *See infra* text accompanying notes 125-26; *see also* Sorkin, *supra* note 20, at 355.

of dealing with spam.¹⁰⁰ An e-mail user manually filters out spam by reviewing all of her messages, deleting any unwanted messages, and keeping desirable ones.¹⁰¹ When an e-mail user accesses her in-box, she sees the message headers of her unread messages.¹⁰² The message header includes the time and date the message was sent, the e-mail address from which the message originated, and the subject of the message.¹⁰³ Ideally, the e-mail user could, without having to open them, quickly delete the messages from unknown senders or messages about subjects of no interest to her.¹⁰⁴ Unfortunately, spammers commonly use misleading “from” and “subject” headers in their messages in order to get e-mail users to open and read a message that they would otherwise delete.¹⁰⁵ An e-mail user risks inadvertently deleting an important message if she deletes a message with an ambiguous subject line without first reading it.¹⁰⁶ As a result, manual filtering is a time-consuming exercise; it takes just one mouse click to delete a single message, but when the average e-mail user receives more than sixty spam messages each day,¹⁰⁷ the aggregate amount of time deleting unwanted messages is significant.¹⁰⁸ Another drawback of manual filtering has to do with the limited storage space in most e-mail accounts.¹⁰⁹ If an e-mail user’s in-box fills up with spam messages, exceeding her storage quota before she has a chance to filter out the unwanted messages,

100. See SCHWARTZ & GARFINKEL, *supra* note 16, at 74.

101. *See id.*

102. *See id.* at 49.

103. *Id.*

104. *See id.* at 74.

105. See FED. TRADE COMM’N, *supra* note 90, at 7 (estimating that forty-four percent of spam contains false information in the “from” or “subject” fields in the message header). Spammers typically alter header information to make it appear as though the message is from someone the recipient knows. FALLOWS, *supra* note 2, at 11. Spam subject lines are frequently made to look as though the message is in response to an inquiry from the recipient. *Id.* Alternatively, the subject line will be cryptic or vague, making it impossible for the recipient to determine the message’s content without opening it. *See id.*

106. Sorkin, *supra* note 20, at 346 n.97.

107. See FALLOWS, *supra* note 2, at 7 (noting that America Online reports that its average in-box receives sixty-seven spam messages daily); see also MCWILLIAMS, *supra* note 61, at 95 (describing how one e-mail user received more than 100,000 spam messages over two days).

108. SCHWARTZ & GARFINKEL, *supra* note 16, at 6. It takes about four seconds for an e-mail user to determine that a message is spam and to delete it. If one million people receive the same message, and each takes four seconds to filter it manually, the cost is about one month in human effort. *Id.*

109. *Id.* at 75.

desirable messages will be returned to their senders as undeliverable.¹¹⁰

2. Software Filters

As early as 1996, America Online (AOL) began filtering incoming messages to block spam.¹¹¹ Today, ISPs' filters block billions of messages each day before they reach users' in-boxes.¹¹² Software filters vary in the way they function, but they all share the goal of blocking spam before it reaches the end user.¹¹³ Some ISPs block all messages from known spammers.¹¹⁴ Other filters use sophisticated pattern-matching parameters to identify and block likely spam messages.¹¹⁵ These filters can analyze the content of a message and determine whether it is spam.¹¹⁶ No matter how good software filters are, programmers are always playing catch-up with the spammers.¹¹⁷ Because spammers are constantly finding new ways to evade filters, the software must be constantly monitored and updated.¹¹⁸ The biggest problem with filtering is the risk of "false positives."¹¹⁹ Software filters can misidentify and delete a desirable message as spam if the message's header or subject line contains a keyword the filter has

110. *Id.*

111. *Id.* at 27. AOL's first filter gave users three choices: 1) receive all e-mail; 2) receive no junk e-mail; or 3) receive no e-mail at all. *Id.* AOL determined what constituted "junk" e-mail to be blocked by the filter. *See id.*

112. *See* Jonathan Krim, *Spam's Cost to Business Escalates*, WASH. POST, Mar. 13, 2003, at A1 (noting that AOL blocks one billion messages each day); *see also* Gates, *supra* note 56 (stating that MSN and Hotmail filters block 2.4 billion messages each day).

113. Sorkin, *supra* note 20, at 346-47.

114. *See* SCHWARTZ & GARFINKEL, *supra* note 16, at 141; *see also* Media3 Technologies, LLC v. Mail Abuse Prevention System, LLC, No. 00-CV-12524-MEL, 2001 U.S. Dist. LEXIS 1310, at *4 (D. Mass. Jan. 2, 2001) (describing a "blackhole list" of known spammers compiled and disseminated by Mail Abuse Prevention System, a non-profit ISP).

115. *See* SCHWARTZ & GARFINKEL, *supra* note 16, at 139.

116. *See* Swidey, *supra* note 15, at 14-15 (describing Bayesian filters based on the theories of 18th-century British mathematician Thomas Bayes).

117. *See id.* at 15.

118. *See* Krim, *supra* note 112. Because of the constant need for adjustment, the use of software filters to fight spam has been compared to "plugging a water-main break with chewing gum." *Id.*

119. *See* Lemke, *supra* note 93 (noting that thirty percent of employees reported missing an important message because of e-mail filtering). E-mail users who practice manual filtering can also accidentally delete desirable messages. *See* Gross, *supra* note 81. Bruce Goldberg, who blames spammers for putting his on-line record store out of business, said that he had to filter out fifteen spam messages for every one legitimate message. "Even as careful as I was, I would still lose customers by accidentally deleting their messages." *Id.*

associated with spam. In one extreme example of the potential drawbacks of software filtering, messages containing the word “specialist” were being blocked by one company’s e-mail filtering software.¹²⁰ Puzzled programmers finally realized that the word contains the letters “cialis,” which the filter recognized as Cialis, the name of a popular erectile dysfunction medication—a product frequently advertised by spammers.¹²¹

3. Commercial Do-Not-Spam Lists

Some companies, seeing opportunity in the absence of regulation, have begun to offer to register consumers on private “no-spam” lists—for a fee.¹²² Proprietors of these lists claim that they can reduce the amount of spam that subscribers receive.¹²³ These services have been criticized, however, as ineffective at best, and fraudulent at worst.¹²⁴

4. Vigilante Tactics

Some e-mail users have become so frustrated by the constant stream of spam flowing into their in-boxes that they have gone on the offensive.¹²⁵ Vigilante tactics used against spammers have included e-mail bombs, blacklisting, and even death threats.¹²⁶ The questionable legality of these approaches aside, vigilante tactics are ineffective because spammers are

120. Mike Cassidy, *Sending E-Mail Can Be a Struggle if Your Name Has a 4-Letter Word*, SAN JOSE MERCURY NEWS (Cal.), Feb. 24, 2004, at 1C, available at <http://www.siliconvalley.com/mld/siliconvalley/8026783.htm>.

121. *Id.* Craig Cockburn (pronounced “Co-burn”) is another innocent victim of spammers. After twenty-one years of using e-mail without incident, he has had to abandon it as a means of communication. Too many e-mail filters block messages he sends because the software recognizes the first four letters of his last name as a vulgar term for a part of the male anatomy. He can no longer send messages with confidence that they will reach their destination. “Quite legitimate e-mail from quite legitimate people is being bounced [by filters].” *Id.*

122. Amit Asravala, *Paying Spammers Not to Spam*, WIRED NEWS, Sept. 15, 2003, at <http://www.wired.com/news/business/0,1367,60431,00.html>.

123. *Id.*

124. *Id.* See also Press Release, Federal Trade Commission, Sham Site Is a Scam: There Is No “National Do Not E-Mail Registry,” (Feb. 12, 2004) at <http://ftc.gov/opa/2004/02/spamscam.htm> (describing a fraudulent Web site, unsub.us, which claimed to be an official government do-not-spam registry).

125. Swidey, *supra* note 15, at 30. Minh Nguyen, a bulk e-mailer, was flooded with junk mail—electronic and postal—shortly after he began transmitting mass e-mailings; his recipients were taking revenge. *Id.*

126. See CANTER & SIEGEL, *supra* note 14, at 24; see also MCWILLIAMS, *supra* note 61, at 21-25 (describing how the vigilante tactics of anti-spam hackers drove Sanford Wallace, one of the most prolific spammers, from the Internet).

2005]

CAN-SPAM ACT OF 2003

975

becoming more and more elusive. An e-mail user bent on exacting revenge on a spammer will have a hard time finding him. And anti-spammers who have taken steps to curtail the activities of spammers have found themselves targets of defamation lawsuits and even threats of violence.¹²⁷ Because many spammers transmit their messages from “highjacked” addresses belonging to innocent third parties, an anti-spam vigilante may unknowingly take out his wrath on another spam victim.¹²⁸

II. THE CAN-SPAM ACT OF 2003

On December 16, 2003, President Bush signed into law the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003.¹²⁹ The Act, which is also known as the CAN-SPAM Act of 2003,¹³⁰ went into effect on January 1, 2004,¹³¹ and is the first federal statute

127. See McWILLIAMS, *supra* note 61, at 69, 212 (describing spammers’ threats against an anti-spam activist who went by the alias “Shiksaa”).

128. FALLOWS, *supra* note 2, at 12. Innocent victims of e-mail address hijacking often find themselves on the receiving end of anti-spam vigilante tactics. One such victim described his encounters with anti-spammers in the following way:

A spammer recently sent out UCE with forged sender information indicating that I sent the mail from a personal email account I maintain. I suffered a deluge (thousands) of bounced emails, death threats, complaints, and removal requests in the short span of time it took me to notice and disable that email account. Consequently, I have been forced to retire the email address from use and all mail to it is now discarded. I am unable to receive legitimate correspondence as a result. I have no reason to believe that I was personally singled out but rather that my address was simply chosen at random by the marketer where the UCE was crafted.

Id.

129. Jennifer 8. Lee, *Bush Signs Law Placing Curbs on Bulk Commercial E-Mail*, N.Y. TIMES, Dec. 17, 2003, at C4. The Act was passed by the Senate on October 22, 2003, by a vote of 97-0. 149 CONG. REC. S13,176 (daily ed. Oct. 23, 2003). The only senators not voting were Senator Inouye of Hawaii, who was absent due to illness, Senator Kerry of Massachusetts and Senator Edwards of North Carolina, both of whom were campaigning for the Democratic Presidential nomination. U.S. SENATE, *U.S. Senate Roll Call Votes 108th Congress – 1st Session*, available at http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=108&session=1&vote=00404 (last visited Apr. 12, 2005). The Act was passed by the House of Representatives on November 22, 2003, by a vote of 392-5. U.S. HOUSE OF REPRESENTATIVES, *Final Vote Results for Roll Call 671*, available at <http://clerk.house.gov/evs/2003/roll671.xml> (last visited Apr. 12, 2005).

130. CAN-SPAM Act of 2003, Pub. L. No. 108-187 § 1, 117 Stat. 2699.

131. *Id.* § 16.

to regulate unsolicited commercial e-mail.¹³² Prior to CAN-SPAM's enactment, commercial e-mail was regulated by a collection of laws passed in more than two-thirds of the states.¹³³ CAN-SPAM preempts those state laws and creates a single framework for the regulation of commercial e-mail.¹³⁴

The Act makes it a crime to send unsolicited commercial e-mail containing fraudulent header information;¹³⁵ it prohibits certain methods of generating e-mail address lists;¹³⁶ it creates regulations requiring the inclusion of certain identifying information in all commercial e-mail;¹³⁷ it prohibits the transmission of commercial e-mail to recipients who have opted out of receiving further communication from the sender;¹³⁸ and it directs the Federal Trade Commission (FTC) to develop a plan for implementing a national Do-Not-E-Mail registry.¹³⁹ The Act charges the Department of Justice with the enforcement of its criminal provisions; the FTC is responsible for enforcement of the Act's regulatory provisions.¹⁴⁰

This section will discuss the state statutes enacted prior to the CAN-SPAM Act, and will describe the CAN-SPAM Act's provisions.

A. State Legislation Prior to the CAN-SPAM Act

Before the enactment of the federal CAN-SPAM Act, commercial e-mail was regulated by a collection of state laws.¹⁴¹ In 1997, Nevada became the first state to pass an anti-spam law,¹⁴² and by 2003, thirty-six states had passed anti-spam statutes of their own.¹⁴³ While the specific provisions in

132. 149 CONG. REC. S13,019 (daily ed. Oct. 22, 2003) (statement of Sen. McCain).

133. See David E. Sorkin, *Spam Laws*, at <http://www.spamlaws.com>. (last visited Apr. 12, 2005) [hereinafter Sorkin Web site]. Professor Sorkin's Web site includes the text of all state anti-spam laws. See *id.*

134. 15 U.S.C.A. § 7707(b) (West Supp. 2004); see also 149 CONG. REC. S13,023 (daily ed. Oct. 22, 2003) (statement of Sen. Wyden).

135. 18 U.S.C.A. § 1037 (West Supp. 2004).

136. 15 U.S.C.A. § 7704(b).

137. See *id.* §§ 7704(a)(3), (a)(5).

138. See *id.* § 7704(a)(4).

139. See *id.* § 7708.

140. See *id.* §§ 7703(c)(2), 7706(a).

141. 149 CONG. REC. S13,023 (daily ed. Oct. 22, 2003) (statement of Sen. Wyden).

142. Prince, *supra* note 8.

143. See Sorkin Web site, *supra* note 133. The states that have passed anti-spam laws are Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Minnesota, Missouri, Nevada, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming. *Id.*

these laws vary widely, most of the statutes share two common goals: (1) eliminating fraud in commercial e-mail, and (2) reducing the overall volume of spam received by e-mail users.¹⁴⁴ State anti-spam statutes share several common provisions aimed at achieving these goals.¹⁴⁵

State anti-spam laws attempt to reduce substantially fraudulent commercial e-mail by requiring senders to reveal their true identities to recipients.¹⁴⁶ The most common provision aimed at eliminating fraudulent e-mail, adopted by thirty-one states, is a prohibition on false header information.¹⁴⁷ Six states also require the inclusion of a valid postal address in all commercial e-mail as an additional means of verifying the sender's identity.¹⁴⁸ State anti-spam statutes not only seek to ensure that recipients know who is sending the message, but they also attempt to guarantee that the message's subject line accurately portrays the message's content.¹⁴⁹ Fourteen states prohibit falsifying e-mail subject lines to trick the recipient into opening a message.¹⁵⁰

As for reducing the volume of spam flowing into e-mail users' inboxes, many state statutes require that senders include a functioning "opt-out" process, and mandate the use of identifying "tags" in the subject lines of commercial e-mail messages.¹⁵¹

Twenty-one state statutes require that the sender of commercial e-mail provide the recipient with a simple, no-cost means of indicating the desire to be excluded from future mailings.¹⁵² The sender must comply by removing the recipient from its mailing list.¹⁵³

Sixteen state statutes require senders of commercial e-mail to include a specific identifying "tag" in the message's subject line.¹⁵⁴ The most common tag required by state statute is "ADV," indicating that the message is an advertisement.¹⁵⁵ These tags can reduce the volume of spam by facilitating efficient filtering.¹⁵⁶ An e-mail user can quickly scan the subject

144. Kendrick, *supra* note 21, at 571.

145. See Sorkin Web Site, *supra* note 133.

146. See Kendrick, *supra* note 21, at 569.

147. *Id.*

148. *Id.*

149. *Id.*

150. *Id.*

151. *Id.* at 570.

152. Kendrick, *supra* note 20, at 570.

153. *Id.*

154. *Id.*

155. See UNSPAM, *Spam Laws Grid*, at http://www.unspam.com/fight_spam/information/spam_laws.html (last visited Apr. 12, 2005) (noting that eighteen state statutes require the use of the ADV tag in the subject line of commercial e-mail messages).

156. See Kendrick, *supra* note 21, at 570.

lines of unopened messages in her in-box, and if she wishes, she can delete all messages with the “ADV” tag without even opening the messages. This eliminates the need to open all messages received for fear of accidentally deleting a message from a family member or business associate. Tags can also be used to filter out spam even before the messages reach the e-mail user’s in-box. A setting in the user’s e-mail program, or even at the ISP level, can instruct software to delete all messages preceded by “ADV.” This would encourage more accurate filtering, reducing the number of spam messages that get past the filter, as well as limiting the number of false positives.¹⁵⁷

Some states have incorporated criminal provisions in their anti-spam legislation.¹⁵⁸ For example, a Virginia law makes it a felony to send more than 10,000 spam messages in a single day or to send more than 100,000 messages in a thirty-day period.¹⁵⁹ The nation’s first arrest under a criminal anti-spam law was made in December 2003, when two men were indicted in Virginia after AOL received more than 100,000 complaints in a single month from members who received spam from the men.¹⁶⁰ The men face five years in prison and \$2,500 each in fines, as well as possible forfeiture of any money they made from their spamming activities.¹⁶¹

In September 2003, the California legislature passed what would have been the most restrictive anti-spam statute in the nation.¹⁶² This law, which would have gone into effect on January 1, 2004, but for preemption by CAN-SPAM, prohibited sending *any* unsolicited commercial e-mail to a California e-mail address, and permitted individual consumers to sue spammers for damages of up to one million dollars.¹⁶³ Unlike other state anti-spam laws, the California law takes an “opt-in” approach to the spam problem.¹⁶⁴ Under the California law, a sender of commercial e-mail cannot initiate contact with an e-mail user unless the recipient requests the information, or if the parties have a pre-existing business relationship.¹⁶⁵ On-line marketers unanimously panned the California law, and mobilized

157. See *supra* text accompanying notes 100-121 (discussing filtering and the risk of inadvertently deleting desirable messages).

158. See Saul Hansell, *Virginia Indicts 2 Under Antispam Law*, N.Y. TIMES, Dec. 12, 2003, at C4.

159. See VA. CODE ANN. § 18.2-152.3:1(B) (Michie 2004).

160. See Hansell, *supra* note 158.

161. See *id.*

162. See Jonathan Krim, *Calif. Gets Strictest Spam Law in U.S.*, WASH. POST, Sept. 25, 2003, at E6.

163. See *id.*; see also CAL. BUS. & PROF. CODE §§ 17529.2, 17529.8 (West 2004).

164. See Krim, *supra* note 162.

165. See *id.*

2005]

CAN-SPAM ACT OF 2003

979

to promote the passage of federal commercial e-mail regulations.¹⁶⁶ Because of its sweeping ban on unsolicited commercial messages, and its implications for interstate commerce, the California law, had it not been preempted by CAN-SPAM, would surely have faced constitutional challenges.¹⁶⁷

B. What the CAN-SPAM Act Does

1. Criminal Liability

The CAN-SPAM Act criminalizes certain techniques adopted by spammers to evade software filters and to conceal their identities.¹⁶⁸ Specifically, the Act outlaws five methods of bypassing anti-spam technology.¹⁶⁹ First, the Act prohibits spammers from hacking into another

166. See Prince, *supra* note 8.

167. See Declan McCullagh, *California Spam Law May Face Court Challenge*, CNETNEWS.COM, Sept. 24, 2003, at http://news.com.com/2100-1024_3-5082049.html?tag=prntfr (last visited Apr. 12, 2005); see also Prince, *supra* note 8.

It's easy to remember the California law, which really inspired the passage of this federal law, as kind of a martyr that was struck down before its time, that would have saved us all from the problem of spam. But the reality is, the only reason that the marketers pushed so hard to push CAN-SPAM to get it passed was because they didn't want to pay the legal bills to strike down the California law. It almost certainly would have been found unconstitutional.

Id.

168. See 149 CONG. REC. S15,946 (daily ed. Nov. 25, 2003) (statement of Sen. Leahy). The criminal provisions in the Act were originally introduced by Senators Leahy and Hatch as the Criminal Spam Act of 2003, and were added to CAN-SPAM as an amendment in October 2003. See *id.*

169. 18 U.S.C.A § 1037(a) (West Supp. 2004). The Act provides for punishment for [w]hoever in or affecting interstate or foreign commerce, knowingly—

(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer,

(2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages,

(3) materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages,

(4) registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and

person's computer, either by a password, or by means of software installed on the remote computer via a Trojan Horse,¹⁷⁰ and sending spam from the remote computer's Internet Protocol (IP) address.¹⁷¹ Second, it is a crime to take advantage of an "open" network server¹⁷² for the purpose of relaying spam with the intent of deceiving ISPs or recipients as to the origin of the message.¹⁷³ Third, spammers may not materially falsify the header information¹⁷⁴ on multiple commercial e-mail messages.¹⁷⁵ Fourth, the

intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or

(5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses....

Id.

170. Trojan Horses are software programs with legitimate functions, but that also include damaging codes hidden within the program. The computer user is tricked into installing the seemingly innocuous program, and once installed, the program allows unauthorized users to access the system. See Robert Ditzion, Elizabeth Geddes & Mary Rhodes, *Computer Crimes*, 40 AM. CRIM. L. REV. 285, 288 n.17 (2003). The name is an analogy to the giant wooden horse the Greeks gave as a gift to the Trojans in Homer's *Iliad*. The Trojans did not know that Greek soldiers were hiding inside the hollow statue. Under cover of darkness, the soldiers emerged, and opened the city gates to their countrymen waiting outside to conquer the city. See Pete Singer, Comment, *Mounting a Fair Use Defense to the Anti-Circumvention Provisions of the Digital Millennium Copyright Act*, 28 U. DAYTON L. REV. 111, 123 n.95 (2002).
171. 18 U.S.C.A. § 1037(a)(5); see also 149 CONG. REC. S15,946 (daily ed. Nov. 25, 2003) (statement of Sen. Leahy).
172. Some server administrators make their servers readily available for the transfer of e-mail and files. Spammers frequently exploit these open networks as a conduit for relaying spam and disguising their identities. See 149 CONG. REC. S15,946 (daily ed. Nov. 25, 2003) (statement of Sen. Leahy).
173. 18 U.S.C.A. § 1037(a)(3); see also 149 CONG. REC. S15,946 (daily ed. Nov. 25, 2003) (statement of Sen. Leahy).
174. The Act specifically defines "header information" as "the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message." 15 U.S.C.A. § 7702(8) (West Supp. 2004).
175. 18 U.S.C.A. § 1037(a)(3). The "materiality" requirement in the header falsification provision was based on a recommendation by the Department of Justice, and imposes a burden on the prosecution to show that the header information was concealed or altered in a manner that would impair the ability of the recipient, or another party, to identify the sender. 149 CONG. REC. S15,946 (daily ed. Nov. 25, 2003) (statement of Sen. Leahy).

statute bans the practice of creating multiple e-mail accounts or domain names, or using information that materially falsifies the identity of the registrant, for the purpose of sending multiple unsolicited commercial e-mails.¹⁷⁶ Finally, the Act prohibits falsely representing oneself as the authorized user of a block of IP addresses for the purpose of using those addresses for the transmission of spam.¹⁷⁷

The Act provides for fines and imprisonment of up to five years for persons found guilty of violating these provisions.¹⁷⁸ The severity of the punishment can be increased based on the volume and frequency of spam transmitted, and the law provides for harsher punishment for spam “kingpins” and recidivists.¹⁷⁹ Also, anyone convicted under the criminal provisions of the CAN-SPAM Act may be forced to forfeit gains realized from illegal spamming, and the equipment used to conduct that activity.¹⁸⁰

The criminal provisions of the CAN-SPAM Act are viewed by some as its most important component.¹⁸¹ The Act’s congressional sponsors hope that the risk of criminal prosecution will deter spammers and reduce the flow of unwanted e-mail into computer users’ in-boxes.¹⁸²

2. Regulation of Commercial E-Mail

In addition to providing for criminal liability for certain fraudulent spamming practices, CAN-SPAM also establishes regulations regarding the transmission and content of all commercial e-mail,¹⁸³ as well as prohibiting

176. 18 U.S.C.A. § 1037(a)(4). This practice is called “account churning,” and involves the use of automated programs which register large numbers of e-mail accounts and send batches of spam from each account in turn. 149 CONG. REC. S15,946-47 (daily ed. Nov. 25, 2003) (statement of Sen. Leahy).

177. 18 U.S.C.A. § 1037(a)(5).

178. *Id.* § 1037(b); *see also* 149 CONG. REC. S15,947 (daily ed. Nov. 25, 2003) (statement of Sen. Leahy).

179. 18 U.S.C.A. § 1037(b); *see also* 149 CONG. REC. S15,947 (daily ed. Nov. 25, 2003) (statement of Sen. Leahy).

180. 18 U.S.C.A. § 1037(c).

181. 149 CONG. REC. H12,192 (daily ed. Nov. 21, 2003) (statement of Rep. Sensenbrenner). “The criminal provisions contained in this legislation are central to its purpose and to its effectiveness.” *Id.*

182. 149 CONG. REC. S13,023 (daily ed. Oct. 22, 2003) (statement of Sen. Wyden); *see also id.* at S15,944 (daily ed. Nov. 25, 2003) (statement of Sen. Schumer). “Spammers: Be put on notice. [When the CAN-SPAM Act goes into effect] you will be committing a criminal act if you do what you are doing now. With this bill, Congress is saying that if you are a spammer, you can wind up in the slammer.” *Id.*

183. The Act defines “commercial electronic mail message” as “any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose).” 15 U.S.C.A. § 7702(2)(A) (West Supp. 2004). The Act

certain methods of acquiring e-mail addresses for commercial mailing lists.¹⁸⁴

The Act prohibits initiating the transmission of a commercial e-mail message, or a transactional or relationship message, which contains header information that is materially false or misleading.¹⁸⁵ Senders of commercial messages may not use subject lines that mislead the recipient about the content or subject matter of the message.¹⁸⁶ The Act sets a standard for

specifically excludes “transactional or relationship messages” from the definition of commercial electronic mail. *Id.* § 7702(2)(B). A transactional or relationship message is defined as

an electronic mail message the primary purpose of which is—

(i) to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender;

(ii) to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient;

(iii) to provide—

(I) notification concerning a change in the terms or features of;

(II) notification of a change in the recipient’s standing or status with respect to; or

(III) at regular periodic intervals, account balance information or other type of account statement with respect to, a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender;

(iv) to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or

(v) to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender.

Id. § 7702(17)(A). The drafters of CAN-SPAM were fully aware that regulation of spam could implicate the First Amendment. Consequently, the Act does not affect charitable, political, or religious messages. 149 CONG. REC. S15,946 (daily ed. Nov. 25, 2003) (statement of Sen. Leahy). “[W]e must not forget that spam, like more traditional forms of commercial speech, is protected by the first amendment.” *Id.*

184. *See infra* text accompanying notes 199-205.

185. 15 U.S.C.A. § 7704(a)(1). The prohibition on false or misleading header information includes header information which is “technically accurate,” but which identifies an e-mail address, domain name or IP address that the sender accessed through fraudulent means. *Id.* § 7704(a)(1)(A).

186. *Id.* § 7704(a)(2).

determining whether a subject line is misleading.¹⁸⁷ If the sender knows, or has reason to know, that the subject line “would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message,” it is in violation of the Act.¹⁸⁸

The CAN-SPAM Act requires that all commercial e-mail messages include “clear and conspicuous identification that the message is an advertisement or solicitation.”¹⁸⁹ Notably, the law does not spell out what form such an “identification” must take in order to be in compliance with the Act.¹⁹⁰ Commercial e-mail messages must include a “valid physical postal address of the sender.”¹⁹¹

CAN-SPAM places restrictions on commercial e-mail containing sexually oriented material.¹⁹² The Act requires that any commercial e-mail message containing sexually oriented material must include in its subject heading clearly identifiable marks or notices.¹⁹³ The purpose of these marks is to inform the recipient of the message’s content, and to facilitate filtering of these messages.¹⁹⁴

The Act requires that senders of commercial e-mail give recipients an

187. *See id.*

188. *Id.*

189. *Id.* § 7704(a)(5)(A)(i).

190. Anti-spam activists were disappointed that Congress declined to adopt provisions in many state laws requiring that commercial e-mails include the tag “ADV” in the subject line. *See infra* text accompanying notes 281-89.

191. 15 U.S.C.A. § 7704(a)(5)(A)(iii). The Act defines a “sender” as “a person who initiates [a commercial electronic mail message] and whose product, service, or Internet website is advertised or promoted by the message.” *Id.* § 7702(16)(A).

192. The Act defines “sexually oriented material” as “any material that depicts explicit sexual conduct . . . unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters.” *Id.* § 7704(d)(4). Some foresee that this definition could be troublesome. Senator Leahy, who supported the Act, expressed concern that the “definition of ‘sexually oriented material’ . . . seems overly broad.” 149 CONG. REC. S15,947 (daily ed. Nov. 25, 2003) (statement of Sen. Leahy).

193. 15 U.S.C.A. § 7704(d)(1)(A). The Act does not expressly prescribe the form that these “marks or notices” will take. Instead, Congress gave the FTC 120 days from the effective date of the Act to “prescribe clearly identifiable marks or notices to be included in or associated with commercial electronic mail that contains sexually oriented material.” *Id.* § 7704(d)(3). In the same way that anti-spam activists were displeased by Congress’s failure to adopt the “ADV” tag for all commercial e-mail, they were also unhappy that Congress chose not to include in the Act itself a requirement that all sexually-explicit spam include a tag like “ADLT” as required by some state laws. *See infra* text accompanying notes 291-97.

194. 15 U.S.C.A. § 7704(d)(3).

opportunity to “opt out” of receiving future messages. All commercial e-mail messages must include a “clear and conspicuous notice of the opportunity ... to decline to receive further commercial electronic mail messages from the sender.”¹⁹⁵ The message must include a link to a functioning return e-mail address, or another Internet-based mechanism for requesting to be removed from the sender’s mailing list.¹⁹⁶ This return address must be capable of receiving such requests for at least thirty days after the message is sent.¹⁹⁷ Once a recipient requests to be removed from the sender’s mailing list, it is unlawful for the sender, or anyone acting on the sender’s behalf, to send any additional commercial e-mail messages to the recipient.¹⁹⁸

In addition to regulations about the transmission and content of commercial e-mail, CAN-SPAM also prohibits certain methods of acquiring e-mail addresses for the purpose of building commercial mailing lists.¹⁹⁹ Specifically, the Act prohibits generating e-mail address lists through address harvesting and dictionary attacks.²⁰⁰ Address harvesting is a process by which spammers deploy specially-designed software programs to search the Internet for e-mail addresses embedded in the code of Web pages and other files.²⁰¹ The Act requires that, in order to be fully protected from the address harvesting ban, a Web site or on-line service must post a notice indicating that any addresses maintained on that site are not to be used to initiate electronic mail messages.²⁰² Dictionary attacking involves programming a computer to systematically transmit messages to sequential e-mail addresses, or to common names, with the expectation that a portion of the addresses generated will be actual e-mail addresses.²⁰³ For example, a spammer might set his dictionary attack to attempt to transmit messages to different permutations of the surname “Smith” at the aol.com domain. The computer would then send messages to asmith@aol.com,

195. *Id.* § 7704(a)(5)(A)(ii).

196. *Id.* § 7704(a)(3)(A).

197. *Id.* § 7704(a)(3)(A)(ii).

198. *Id.* § 7704(a)(4)(A). The Act gives the sender ten days to comply with the recipient’s opt-out request. *Id.* § 7704(a)(4)(A)(i).

199. *Id.* § 7704(b).

200. 15 U.S.C.A. § 7704(b)(1).

201. *Verizon Online Services v. Ralsky*, 203 F. Supp. 2d 601, 607 (E.D. Va. 2002).

202. 15 U.S.C.A. § 7704(b)(1)(A)(i). In order for harvested addresses to fall under the Act’s prohibition, the Web site or on-line service must include “a notice stating that the operator of such website or online service will not give, sell, or otherwise transfer addresses maintained by such website or online service to any other party for the purposes of initiating, or enabling others to initiate, electronic mail messages.” *Id.*

203. *MCWILLIAMS*, *supra* note 61, at 302.

bsmith@aol.com, csmith@aol.com, and so on.²⁰⁴ Many of the addresses generated by the dictionary attack will not be valid, but there is a good likelihood that many of them will be valid. Since the entire process is automated, the cost to the spammer is low.²⁰⁵

3. Do-Not-E-Mail Registry

The CAN-SPAM Act directs the Federal Trade Commission (FTC) to develop a plan for the establishment of a national “Do-Not-E-mail Registry” within six months of the enactment of CAN-SPAM.²⁰⁶ The Act authorizes the FTC to implement its plan and roll out the registry without further congressional authorization no sooner than nine months after the enactment of CAN-SPAM.²⁰⁷

The Do-Not-Spam list was added to the CAN-SPAM Act in an amendment proposed by New York Senator Charles Schumer, in October 2003.²⁰⁸ The concept of compiling a list of e-mail addresses and domains that are off-limits for spammers was inspired by the popularity of the national Do-Not-Call list²⁰⁹ which went into effect a few weeks before the

204. See Caroline E. Mayer & Ariana Eunjung Cha, *Making Spam Go Splat*, WASH. POST, June 9, 2002, at H1.

205. In addition to the Act’s prohibition against address harvesting and dictionary attacks, e-mail users and Web site administrators can protect their addresses against these tactics by “munging” their addresses. See SCHWARTZ & GARFINKEL, *supra* note 16, at 69. When an e-mail user munges her address, she replaces the address with one that does not work but could be easily ascertained by an actual human being. For example, an e-mail user whose address is jsmith@aol.com could munge it by changing it to jsmith@delete.aol.com. She could then include instructions in her signature to remove the “delete” before replying to her message. If the address is harvested, it will be ineffective. See *id.*

206. 15 U.S.C.A. § 7708(a).

207. *Id.* § 7708(b).

208. See 149 CONG. REC. S13,024 (daily ed. Oct. 22, 2003) (statement of Sen. Schumer).

209. The Do-Not-Call registry was established by the FTC as an amendment to the Telemarketing Sales Rules. *FTC v. Mainstream Mktg. Servs.*, 345 F.3d 850, 851 (10th Cir. 2003). The Do-Not-Call registry includes “telephone numbers of consumers who have indicated that they do not wish to receive unsolicited telephone calls from commercial telemarketers, and it prohibits those telemarketers from making sales calls to consumers on the list.” *Id.* The FTC began accepting registrations for the Do-Not-Call list in June 2003. Matt Richtel, *National Do-Not-Call Registry Overwhelmed by Eager Public*, N.Y. TIMES, June 28, 2003, at C2. By the registry’s October 1, 2003 effective date, more than fifty million consumers had added their telephone numbers to the list. Matt Richtel, *No-Call List Dealt Setback in Court Ruling*, N.Y. TIMES, Sept. 25, 2003, at C1. While popular with consumers, the Do-Not-Call list faced legal challenges from the telemarketing industry, which argued that the registry was an unconstitutional restriction on free speech, and that the FTC was not authorized to establish the list. *U.S. Security v. FTC*, 282 F. Supp. 2d 1285,

Do-Not-Spam list was proposed.²¹⁰

Timothy J. Muris, Chairman of the FTC, expressed skepticism about the effectiveness of a Do-Not-Spam list.²¹¹ Muris stated that while the Do-Not-Call registry will significantly reduce the number of telemarketing calls received by consumers, a Do-Not-Spam list would not be successful in limiting the number of unsolicited e-mail messages because most spammers would ignore it.²¹² E-mail experts also worry that if the registry ended up in the wrong hands, it would be a gold mine for spammers.²¹³ The registry could potentially be the largest list of actual e-mail addresses ever compiled.²¹⁴ In order to prevent such security breaches, a Do-Not-Spam registry would operate differently from the Do-Not-Call list.²¹⁵ Telemarketers are required to pay an annual fee to gain access to the Do-Not-Call registry, and three times a year, telemarketers download an updated database of telephone numbers.²¹⁶ By contrast, the Do-Not-Spam list would not be downloaded by e-mail marketers, and would be protected

-
- 1290 (W.D. Okla. 2003); *Mainstream Mktg. Servs. v. FTC*, 283 F. Supp. 2d 1151, 1154 (D. Colo. 2003). Two federal district courts enjoined the FTC from enforcing the Do-Not-Call rules. *U.S. Security*, 282 F. Supp. 2d at 1294; *Mainstream Mktg. Servs.*, 283 F. Supp. 2d at 1171. The Do-Not-Call list was saved by a subsequent congressional grant of express authority for the FTC to promulgate the registry, and a stay of injunction issued by the Tenth Circuit Court of Appeals. See Sheryl Gay Stolberg & Matt Richtel, *Do-Not-Call Listing Remains Up in Air After Day of Twists*, N.Y. TIMES, Sept. 26, 2003, at A1; *FTC v. Mainstream Mktg. Servs.*, 345 F.3d at 860.
210. See 149 CONG. REC. S13,019 (daily ed. Oct. 22, 2003) (statement of Sen. McCain). "If we can implement a Do Not Spam provision which is clearly modeled after the Do Not Call list, I think it will have enormous benefit to all Americans." *Id.*; see also *id.* at H12,192 (daily ed. Nov. 21, 2003) (statement of Rep. Tauzin).
211. See Jonathan Krim, *Head of FTC Opposes Bills to Curb Spam*, WASH. POST, Aug. 20, 2003, at E1. Chairman Muris said that such a registry would be "largely ineffective." *Id.*
212. Timothy J. Muris, Remarks at the Aspen Summit on Cyberspace and the American Dream (Aug. 19, 2003), available at <http://www.ftc.gov/speeches/muris/030819aspen.htm>. Chairman Muris called the Do-Not-Spam list an "intriguing idea," but observed "[t]here is no basis to conclude that a [Do-Not-Spam] list would be enforceable or produce any noticeable reduction in spam. If it were established, my advice to consumers would be: Don't waste the time and effort to sign up." *Id.*
213. See Grover G. Norquist & Tom Readmond, *OutsideView: Do Not Spam? Not So Fast*, UNITED PRESS INT'L (Oct. 28, 2003).
214. See *id.*; see also 149 CONG. REC. S13,025 (daily ed. Oct. 22, 2003) (statement of Sen. Schumer).
215. See 149 CONG. REC. S13,025 (daily ed. Oct. 22, 2003) (statement of Sen. Schumer).
216. See FED. TRADE COMM'N, *Q & A for Telemarketers and Sellers About the Do Not Call Provisions of the FTC's Telemarketing Sales Rule*, available at <http://www.ftc.gov/bcp/online/pubs/alerts/dncbizarlt.htm> (last visited Feb. 21, 2005).

by military-caliber encryption.²¹⁷

Even if it were disregarded, or worse, exploited by spammers, a national Do-Not-Spam list could still be beneficial in the battle against spam. To date, one of the biggest challenges in imposing liability on spammers is the inability of plaintiffs to establish that the spammer is subject to the personal jurisdiction of the court in which the action is instituted.²¹⁸ It is impossible to determine, by simply looking at an e-mail address, where that e-mail user resides.²¹⁹ A registry of e-mail addresses that identifies the geographic location of the address's owner could establish personal jurisdiction.²²⁰ The experience of Washington state is illustrative. More so than in any other state, lawsuits against spammers in Washington have been successful.²²¹ This success may be due in part to the Washington Association of Internet Service Providers Registry (WAISP Registry).²²² The registry, which is co-sponsored by WAISP and the Washington Attorney General's office, provides a means for Washington residents to associate their e-mail address with their physical address, thereby establishing that their e-mail address is protected by the Washington anti-spam statute.²²³ Similarly, if a nationwide e-mail address registry were established, plaintiffs could prove that recipients' e-mail addresses are under the jurisdiction of a particular court, and, by sending messages to those addresses, the sender has availed himself of the benefits and protections of that jurisdiction's laws.²²⁴

In June 2004, the FTC issued its report on the feasibility of implementing a national Do-Not-E-mail registry modeled after the Do-Not-Call registry.²²⁵ The Commission determined that "without a system in place to authenticate the origin of email messages, [a Do-Not-Spam

217. See 149 CONG. REC. S13,025 (daily ed. Oct. 22, 2003) (statement of Sen. Schumer).

218. See Prince, *supra* note 8.

219. See *id.*

220. See *id.*

221. See *id.*; see also, e.g., State v. Heckel, 24 P.3d 404 (Wash. 2001) (upholding a state law prohibiting deceptive spam directed to a Washington resident or initiated from a computer located in Washington).

222. See Prince, *supra* note 8.

223. See WASH. ASSOC. OF INTERNET SERV. PROVIDERS, *WAISP Registry Page*, at <http://registry.waisp.org/> (last visited Feb. 21, 2005).

224. See Prince, *supra* note 8; see also Hanson v. Denckla, 357 U.S. 235, 253 (1958) (holding that, in order to establish personal jurisdiction, there must be "some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws").

225. FED. TRADE COMM'N, *National Do Not Email Registry: A Report to Congress* (2004), available at <http://www.ftc.gov/reports/dneregistry/report.pdf> (last visited Feb. 21, 2005).

registry] would fail to reduce the burden of spam and may even increase the amount of spam received by consumers.”²²⁶ The Commission found that they would be unable to prevent spammers from misusing the registry, thereby making it possible for spammers to exploit it as a means of verifying active e-mail addresses, and targeting children.²²⁷ The Commission concluded that, until the technological marketplace develops reliable authentication software, “any Registry is doomed to fail.”²²⁸

4. Enforcement

Congress designated the Department of Justice to enforce the criminal provisions of the CAN-SPAM Act.²²⁹ The Federal Trade Commission has been named as the primary enforcement agency of the regulatory provisions of the CAN-SPAM Act.²³⁰

The Act gives the FTC broad authority to enforce the regulations against violators. In order to make it easier for the FTC to prevail in court, Congress waived the Act’s “knowledge” requirements when the government seeks injunctive relief.²³¹ The FTC can be granted a cease-and-desist order even if the government cannot prove that a spammer knowingly engaged in conduct prohibited by the Act.²³²

Congress also authorized state attorneys general, and other state officials and agencies to bring a civil action on behalf of the residents of a state when that official or agency has reason to believe that those residents are being harmed or threatened by violations of the CAN-SPAM Act.²³³ Any state authority suing under the Act must first notify the FTC before bringing suit, and the FTC has the right to intervene in any action brought by a state authority.²³⁴ Also, no state actor may bring an action against a defendant named in an action brought by the FTC while that action is

226. *Id.* at i.

227. *Id.*

228. *Id.* at ii.

229. See 15 U.S.C.A. § 7703(c)(2) (West Supp. 2004). “It is the sense of Congress that . . . the Department of Justice should use all existing law enforcement tools to investigate and prosecute those who send bulk commercial e-mail to facilitate the commission of Federal crimes.” *Id.*

230. *Id.* § 7706(a). The Act also authorizes other federal agencies, including the Federal Deposit Insurance Corporation, the Board of the National Credit Union Administration, the Securities and Exchange Commission, the Federal Communications Commission, and the Secretaries of Transportation and Agriculture, to enforce the Act under certain circumstances. See *id.* § 7706(b).

231. 149 CONG. REC. H12,860 (daily ed. Dec. 8, 2003) (statement of Rep. Markey).

232. 15 U.S.C.A. § 7706(e).

233. *Id.* § 7706(f)(1).

234. *Id.* § 7706(f)(5).

pending.²³⁵

Enforcement of CAN-SPAM is not limited to persons who send e-mail. The Act also imputes parties whose products or services are promoted by third party spammers.²³⁶ This provision makes it more likely that the FTC will have successful prosecutions, since it will be easier to locate companies whose products are advertised in spam messages than it is to track down spammers who disguise their identity, and who may be located offshore.

The CAN-SPAM Act also directs the FTC to develop a system of rewarding people who provide the government with information which identifies violators and leads to their successful prosecution.²³⁷

5. Private Cause of Action

Under CAN-SPAM, ISPs that have been adversely affected by a violation of the Act may bring a civil action against the spammer.²³⁸ ISPs may seek injunctive relief or monetary damages. ISPs can recover the greater of actual money damages or statutory damages.²³⁹ Congress decided to limit enforcement of the Act to federal and state agencies and ISPs. Individual consumers may not sue under the Act.²⁴⁰

235. *Id.* § 7706(f)(8).

236. *Id.* § 7705(a); *see also* Prince, *supra* note 8.

237. 15 U.S.C.A. § 7710(1)(A). The Act states that rewards for informants should be “not less than [twenty] percent of the total civil penalty collected.” *Id.* CAN-SPAM’s “bounty system” was proposed by Stanford Law School professor Lawrence Lessig, who was so certain that “deputizing” computer-savvy citizens to track down spammers would greatly reduce the volume of spam, that he vowed to resign from his job if it did not work. McWILLIAMS, *supra* note 61, at 275.

238. 15 U.S.C.A. § 7706(g)(1).

239. *Id.*

240. *See* 149 CONG. REC. H12,193 (daily ed. Nov. 21, 2003) (statement of Rep. Sensenbrenner). “[I]t is not the intent of Congress to allow outsourcing of this truly State function to the plaintiff’s bar.” *Id.* The elimination of the individual cause of action is a key difference between CAN-SPAM and state laws like California’s 2003 anti-spam law. Under that law, an individual e-mail user could potentially sue a spammer and collect damages up to one million dollars. *See supra* text accompanying note 163. Critics of CAN-SPAM were disappointed that Congress limited private-party standing to ISPs. *See* Hitt, *supra* note 65. If spammers had to defend against potentially millions of lawsuits brought by individual consumers, the legal costs would significantly increase the cost of doing business for spammers, cutting into profit margins to the point that spamming would no longer be an attractive marketing tool. One anti-spam activist called this form of distributive justice “death by a thousand paper cuts.” *Id.* Trade groups representing on-line marketers oppose allowing individual consumers to sue senders of unsolicited e-mail. O. Burtch Drake et al., *Congress, Pass National Anti-Spam Legislation NOW or E-commerce Will Be*

6. Preemption of State Laws

One of the stated purposes of CAN-SPAM was to reduce the confusion caused by inconsistent state anti-spam laws, and to create a unified national framework for the regulation of commercial e-mail.²⁴¹ CAN-SPAM supercedes the “patchwork of inconsistent State laws,” and sets out a single standard for dealing with spam.²⁴² By its express language, CAN-SPAM preempts “any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages....”²⁴³ Thus, with a single stroke of his pen, President Bush effectively wiped out anti-spam statutes in more than two-thirds of the states when he signed CAN-SPAM into law. While some spammers did not even attempt to obey prior state laws,²⁴⁴ those e-mail marketers who do wish to comply with the law were pleased to have a single standard to follow.²⁴⁵

CAN-SPAM does not, however, completely obliterate all state anti-spam laws. The Act has important “carve-outs” that give states some

Crippled!, ROLL CALL, Nov. 13, 2003, at B11. In an open letter to Congress, the presidents of the Direct Marketing Association (DMA), the American Association of Advertising Agencies (AAAA), and the Association of National Advertisers (ANA) warned that if a federal anti-spam bill did not limit private-party standing, large and small businesses, including legitimate retailers, would be “socked with major legal bills as frivolous and wasteful lawsuits continue to soar.” *Id.* The letter went on to note that one-third of all private party suits brought under Utah’s anti-spam law were dismissed because the named defendant was not the party responsible for initiating the unsolicited messages. *Id.*

241. 15 U.S.C.A. § 7701(a)(11); *see also* 149 CONG. REC. S13,023 (daily ed. Oct. 22, 2003) (statement of Sen. Wyden). “I believe a State-by-State approach cannot work in this area. The numerous State laws to date certainly have not put in place a coordinated effort against spam.” *Id.*
242. 149 CONG. REC. S13,023 (daily ed. Oct. 22, 2003) (statement of Sen. Wyden). Regulating commercial e-mail under a federal law also eliminates the interstate commerce problems arising from state legislation. *See* Rep. Heather Wilson, *What Can Congress Do to Relieve Consumers of Unwanted Electronic Solicitation?*, ROLL CALL, Mar. 18, 2002, at 10.
243. 15 U.S.C.A. § 7707(b)(1).
244. 149 CONG. REC. S13,023 (daily ed. Oct. 22, 2003) (statement of Sen. Wyden) (noting that “spammers do not even go through the motions of trying” to comply with inconsistent state anti-spam laws).
245. *See* David Firestone & Saul Hansell, *Senate Votes to Crack Down on Some Spam*, N.Y. TIMES, Oct. 23, 2003, at C1. Michael Mayor, president of Netcreations, a New York firm that assembles e-mail marketing lists, said, “I am thrilled beyond words.... Now we will have one standard for responsible e-mail instead of the [thirty-seven] state laws we have now.” *Id.*

flexibility in regulating fraudulent spam.²⁴⁶ The Act also preserves some of the opportunities for individual consumers to protect their rights under other state laws.²⁴⁷

CAN-SPAM does not preempt state anti-spam laws “to the extent that [a state law] prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.”²⁴⁸ This language indicates that provisions in state laws like Virginia’s, which criminalize the use of false information in spam messages, will remain intact.²⁴⁹

The CAN-SPAM Act has no effect on state laws that do not specifically address electronic mail.²⁵⁰ This language seems to indicate that individual consumers, who have no cause of action against spammers under CAN-SPAM, might still be able to protect their rights by bringing suit against spammers under existing statutes or common law causes of action not specific to e-mail. While the possibility of individual private suits against spammers on non-spam theories is encouraging, it is relatively untested.²⁵¹ To date, suits against spammers brought by individuals on legal theories not specific to spam are rare, and have been generally unsuccessful.²⁵²

For example, a Pennsylvania court held that the federal Telephone Consumer Protection Act of 1991 (TCPA) was inapplicable to spam.²⁵³ The TCPA makes it illegal to send unsolicited commercial faxes, and provides a private cause of action for individuals with potential damages of up to \$500 per incident.²⁵⁴ In *Aronson v. Bright-Teeth Now*,²⁵⁵ the recipient of multiple unsolicited e-mail advertisements for teeth-whitening products argued that the TCPA prohibits spam.²⁵⁶ The court rejected the plaintiff’s argument,

246. See John Praed, Address at the 2004 Spam Conference at the Massachusetts Institute of Technology (Jan. 16, 2004) (transcript on file with the author), available at <http://spamconference.org/webcast.html> (webcast only available on-line).

247. See 15 U.S.C.A. § 7707(b)(2).

248. *Id.* § 7707(b)(1).

249. See Praed, *supra* note 246.

250. 15 U.S.C.A. § 7707(b)(2). “This [Act] shall not be construed to preempt the applicability of . . . State laws that are not specific to electronic mail, including State trespass, contract, or tort law . . .” *Id.*

251. See Prince, *supra* note 8.

252. See, e.g., *Aronson v. Bright-Teeth Now, LLC*, No. AR01-6310, 2002 WL 1466477 (Pa. Com. Pl. June 19, 2002); *Intel Corp. v. Hamidi*, 71 P.3d 296 (Cal. 2003).

253. *Aronson*, 2002 WL 1466477.

254. 47 U.S.C. § 227(b) (2000). The TCPA states “it shall be unlawful for any person . . . to use any telephone facsimile machine, computer or other device to send an unsolicited advertisement to a telephone facsimile machine.” *Id.*

255. 2002 WL 1466477.

256. *Id.* at *1-2. The plaintiff argued that the definition of a “telephone facsimile machine”

holding that there are fundamental differences between unsolicited commercial faxes and spam,²⁵⁷ and that Congress only intended the TCPA to regulate faxes, not e-mail.²⁵⁸

Attempts to use the common law tort cause of action of trespass to chattels have achieved mixed results. In 1996, the Court of Appeal of California held, in *Thrifty-Tel v. Beznec*,²⁵⁹ that hacking into another's computer system could constitute a trespass to chattels, even in the absence of physical damage to the computer hardware.²⁶⁰ Courts followed the *Thrifty-Tel* holding²⁶¹ until 2003 when the California Supreme Court held, in *Intel Corp. v. Hamidi*,²⁶² that trespass to chattels "does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning."²⁶³ If other jurisdictions adopt the *Intel* holding and require

in the TCPA—"equipment which has the capacity (A) to transcribe text or images, or both, from paper into an electronic signal and to transmit that signal over a regular telephone line, or (B) to transcribe text or images (or both) from an electronic signal received over a regular telephone line onto paper"—applied to a personal computer equipped with a modem and a printer. *Id.*; see also David E. Sorkin, *Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991*, 45 BUFF. L. REV. 1001, 1002 (1997).

257. See *Aronson*, 2002 WL 1466477, at *1-2. The court noted that the recipient of an unsolicited commercial fax incurs costs of four to twelve cents per page in ink, paper, and wear and tear on the machine, and also, the recipient is deprived of the use of his fax machine until the transmission of the unsolicited fax is complete. *Id.* The recipient of spam, on the contrary, only incurs printing costs if he chooses to print the message, and usually, the transmission of unwanted e-mail messages does not interfere with the use of the recipient's computer. *Id.*
258. See *id.* at *3. It is worth noting, however, that some of the early congressional sponsors of federal anti-spam bills modeled their legislation after the TCPA. See Jonathan Krimm, *Draft of Bill on Mass E-Mail Is Called Weak*, WASH. POST, May 13, 2003, at E01.
259. 46 Cal. App. 4th 1559 (1996).
260. *Id.* at 1566 (holding that "[t]respass to chattel ... lies where an intentional interference with the possession of personal property has proximately caused injury").
261. See, e.g., *eBay, Inc. v. Bidder's Edge*, 100 F. Supp. 2d 1058, 1069-70 (N.D. Cal. 2000) (holding that "electronic signals sent by [Bidder's Edge] to retrieve information from eBay's computer system [were] sufficiently tangible to support a trespass cause of action"); *Hotmail Corp. v. Van\$ Money Pie*, No. C98-20064 JW, 1998 U.S. Dist. LEXIS 10729, at *19-20 (N.D. Cal. 1998) (holding that Hotmail demonstrated a likelihood of success in its trespass to chattels claim against defendant spammers who made unauthorized use of Hotmail's computer networks, causing Hotmail injury "in terms of added costs for personnel ... and in terms of harm to Hotmail's business reputation and goodwill").
262. 71 P.3d 296 (Cal. 2003).
263. *Id.*

evidence of physical damage to the plaintiff's computer hardware, it is unlikely that individual e-mail users will be able to avail themselves of the trespass cause of action in order to get relief from spam.

It is conceivable that individuals could pursue spammers under theories of tort liability other than trespass to chattels, such as breach of contract,²⁶⁴ nuisance,²⁶⁵ fraudulent misrepresentation, and tortious interference with contractual relations.²⁶⁶ However, there is little precedent upon which an individual plaintiff could base a claim on one of these theories against a spammer.²⁶⁷

Many of the players who were particularly active in state anti-spam movements were disappointed by CAN-SPAM's preemptive effect on state laws.²⁶⁸ Some observers expect that there will be fights over whether specific state laws have in fact been preempted.²⁶⁹ These fights may be distracting and unnecessary.²⁷⁰ One attorney active in the fight against spam suggested that, rather than wasting time on infighting over preemption, "it's best to aim the weapon that we have at the spammers and pull the trigger, because it won't take much to knock them down."²⁷¹

264. See Prince, *supra* note 8. Matthew Prince, a professor of law at the John Marshall School of Law, and the founder of Unspam, suggests that Web site operators insert language in their sites' terms of service prohibiting "non-human visitors," like spiders and bots, from harvesting e-mail addresses from the site. Since courts have held that Web site visitors are bound by the site's terms of service, spammers who harvest addresses from a site in violation of those stated terms would be liable to the Web site's owner for breach of contract. See *Register.Com, Inc. v. Verio, Inc.*, 356 F.3d 393, 403 (2d Cir. 2004) ("While new commerce on the Internet has exposed courts to many new situations, it has not fundamentally changed the principles of contract. It is standard contract doctrine that when a benefit is offered subject to stated conditions, and the offeree makes a decision to take the benefit with knowledge of the terms of the offer, the taking constitutes an acceptance of the terms, which accordingly become binding on the offeree.").

265. See Jeremiah Kelman, *E-Nuisance: Unsolicited Bulk E-Mail at the Boundaries of Common Law Property Rights*, 78 S. CAL. L. REV. 363, 387-99 (proposing a cause of action for "e-nuisance," applying common law nuisance principles to the spam problem).

266. See Sorkin, *supra* note 20, at 362.

267. See *id.* at 358 n.158.

268. See Jonathan Krimm, *Anti-Spam Act Signed but Some Are Skeptical*, N.Y. TIMES, Dec. 17, 2003, at A18.

269. See Praed, *supra* note 246.

270. See *id.*

271. *Id.*

C. What the CAN-SPAM Act Does Not Do

1. Opt-In vs. Opt-Out

CAN-SPAM takes a decidedly “opt-out” approach to the spam problem.²⁷² That is, it only becomes unlawful to send unsolicited commercial e-mail messages to a recipient after she has opted out, or informed the sender that she does not wish to receive further messages from the sender.²⁷³ One of the disadvantages of an opt-out system is that it allows every spammer to send at least one e-mail message to every e-mail address.²⁷⁴ In this way, the Act places the burden on the recipients to respond and remove themselves from the spammer’s address list.²⁷⁵ Another drawback to an opt-out approach is the fact that, for years, consumers have been advised not to respond to spam messages under any circumstances—even to unsubscribe.²⁷⁶ Some have suggested that replying to a spam message, or “clicking through” to an opt-out Web page only provides the spammer with confirmation that the message was received, and encourages the spammer to send additional messages.²⁷⁷ If the CAN-SPAM Act’s opt-out provision is to succeed at reducing spam, computer users will need to be educated about the law, and will need to be convinced

272. 149 CONG. REC. S15,947 (daily ed. Nov. 25, 2003) (statement of Sen. Leahy).

273. *Id.*

274. *Id.* Actually, because the Act gives spammers ten days to comply with a recipient’s opt-out request, a spammer could send many messages to an e-mail user within the ten-day grace period without violating the law. 15 U.S.C.A. § 7704(a)(4)(A)(i) (West Supp. 2004).

275. *See* 149 CONG. REC. S15,945 (daily ed. Nov. 25, 2003) (statement of Sen. Leahy).

276. *See id.* An Assistant Attorney General in Vermont advised consumers, “It’s very bad to reply, even to say don’t send anymore. It tells the spammer they have a live address.... The best thing you can do is just keep deleting them.” *Id.* Massachusetts Attorney General Tom Reilly offers similar advice to consumers. *See* MASS. ATTORNEY GEN. TOM REILLY, *AG Reilly’s Tips for Dealing With Spam A.K.A. Unwanted Email*, (Jan. 15, 2004), at <http://www.ago.state.ma.us/sp.cfm?pageid=1552>. “[T]he best way to avoid spam is probably just to ignore it and delete it—if you respond to these messages, the marketers who send them will know that yours is a ‘live’ e-mail account.” *Id.* The American Association of Retired Persons (AARP) also recommends that senior citizens refrain from replying to spam for any reason. SANDY BERGER, AM. ASS’N OF RETIRED PERSONS, *How to Fight Spam*, available at <http://www.aarp.org/computers-howto/Articles/a2003-12-15-fightspam.html> (last visited Apr. 13, 2005).

277. *See* Chris Gaither, *As Antispam Law Hits, No Holiday from Junk E-mail*, BOSTON GLOBE, Jan. 3, 2004, at A1. Some consumers have reported receiving as much as ten times as many messages after requesting to be removed from spammers’ databases. *Id.*

that spammers will honor opt-out requests and not view them as invitations to send more spam.²⁷⁸

Many anti-spam activists were disappointed that Congress did not choose to take an “opt-in” approach.²⁷⁹ Under an opt-in scheme, a sender may not initiate a commercial e-mail message to a recipient unless and until that recipient has first given them permission to do so. It is obvious that an opt-in system would dramatically reduce the volume of spam, however, it would also drastically limit the development of e-commerce and the free flow of information across the Internet. Also, as appealing as an opt-in law may be, it almost surely would be vulnerable to a constitutional challenge.²⁸⁰

2. ADV and ADLT Tags

CAN-SPAM requires that commercial e-mail messages contain a “clear and conspicuous identification that the message is an advertisement or solicitation,”²⁸¹ and prohibits the sending of sexually oriented commercial e-mail messages without “marks or notices” identifying the messages as such.²⁸² The Act is silent, however, on the specifics of these provisions.

Anti-spam activists were disappointed that Congress included an imprecise “clear and conspicuous identification” requirement, and chose not to implement a standard labeling convention for all commercial e-mail, like the ADV tag required by many of the state laws that were preempted by CAN-SPAM. Including a tag, like ADV, in the subject line of all commercial e-mail messages would facilitate the filtering of virtually all unsolicited commercial messages.²⁸³ Direct marketers opposed a requirement of a specific ADV tag for this very reason.²⁸⁴ Small businesses argue that requiring an ADV tag on all commercial e-mail will give an unfair advantage to large, established companies. First, because the tag would not be required on “relationship” or “transaction” messages,²⁸⁵ only

278. See FALLOWS, *supra* note 2, at 24. A significant percentage of e-mail users do not attempt to contact spammers to opt out, either because they believe that their request will not be honored, or because they fear that it will confirm the validity of their e-mail address. See Gaither, *supra* note 277. “Until those unsubscribe links become more reliable, it’s safer to hit delete.” *Id.*

279. See Prince, *supra* note 8.

280. See *id.*

281. 15 U.S.C.A. § 7704(a)(5)(A)(i) (West Supp. 2004).

282. *Id.* § 7704(d)(1)(A).

283. See Kendrick, *supra* note 21, at 574.

284. See *id.*

285. CAN-SPAM expressly excludes these messages from its regulations. 15 U.S.C.A. §

those companies with whom the recipient has an existing consumer relationship will be able to get commercial messages through filters set to delete all messages with the ADV prefix.²⁸⁶ Second, even if messages with the ADV prefix are not automatically filtered out, small businesses will still be stigmatized by the label.²⁸⁷ Critics of the tag have suggested that if a recipient does not already know and trust the sender of a message bearing an ADV tag, the recipient will assume that the message is from a pornographer, or from a party offering “shady” business deals or “body enhancement scams.”²⁸⁸

Congress included a provision in the Act requiring the FTC to study the impact of the use of the ADV tag, and to report their findings within eighteen months.²⁸⁹ This battle in the spam war highlights the fundamental disagreement over the purpose and goal of CAN-SPAM. If the goal of the Act is to reduce the volume of spam at all costs, then the answer is clear: a uniform tag, like ADV, which can be used to filter out *all* unsolicited commercial messages will go a long way toward achieving that goal. If, however, the goal is not to eradicate spam completely, but rather to protect consumers from fraudulent e-mail offers, “clear and conspicuous,” though non-uniform, “identification” will allow e-mail users to quickly identify commercial messages without inhibiting the free flow of information over the Internet or stymieing the development of e-commerce.²⁹⁰

As for sexually oriented messages, the Act orders the FTC, in consultation with the Attorney General, to “prescribe clearly identifiable marks or notices to be included in or associated with” commercial e-mail messages containing sexually oriented material.²⁹¹ In April 2004, the FTC issued its final rule regarding the labeling of e-mail messages containing sexually explicit material.²⁹² The rule requires that all commercial e-mail containing sexually oriented material “include in the subject heading the phrase ‘SEXUALLY-EXPLICIT:’ in capital letters as the first nineteen

7702(2)(B).

286. See Kendrick, *supra* note 21, at 574.

287. See *id.* (calling the ADV tag a “badge of shame”).

288. *Id.*

289. 15 U.S.C.A. § 7710(2).

290. See 149 CONG. REC. H12,194 (daily ed. Nov. 21, 2003) (statement of Rep. Goodlatte) (cautioning against over-regulating commercial e-mail and “taking the information out of the Information Age”); see also *id.* at S13,020 (daily ed. Oct. 22, 2003) (statement of Sen. McCain) (noting that restrictions should not prevent legitimate businesses from servicing their customers).

291. 15 U.S.C.A. § 7704(d)(3) (West Supp. 2004).

292. Label for Email Messages Containing Sexually Oriented Material, 69 Fed. Reg. 21,024 (Apr. 19, 2004).

2005]

CAN-SPAM ACT OF 2003

997

(19) characters at the beginning of the subject line.”²⁹³ The FTC believes that adding this mark in the subject line of commercial e-mail containing sexually oriented material will “effectively aid[] recipients to recognize and filter emails that contain sexually oriented materials.”²⁹⁴ With regard to the body of commercial e-mail messages, the rule also prohibits inclusion of any sexually oriented material in the area that is “initially viewable by the recipient.”²⁹⁵ In other words, the rule requires that if a recipient of an e-mail containing sexually oriented material were to open the message, he would have to take affirmative action, such as “scrolling down,” to view the sexually oriented material.²⁹⁶ The FTC calls this the “electronic brown paper wrapper”—a reference to the type of wrapping often used to send sexually oriented material through the postal mail.²⁹⁷

III. CAN THE LAW SOLVE THE SPAM PROBLEM?

A. Will CAN-SPAM Work?

Even before CAN-SPAM’s enactment, critics predicted that it would be ineffective.²⁹⁸ Some even cautioned that, rather than achieving Congress’s goal of reducing spam, the statute would actually have the opposite effect.²⁹⁹ The law was renamed the “You *Can* Spam” Act by some who argued that the statute’s effect was to legitimize unsolicited commercial e-mail.³⁰⁰ So long as senders refrained from including fraudulent or misleading content, and included the identifying information required by the Act, they could send as many unsolicited commercial messages as they wanted.³⁰¹ The burden is on the recipient, under CAN-

293. *Id.* at 21,033.

294. *Id.* at 21,028.

295. *Id.* at 21,033.

296. *Id.* at 21,031.

297. *Id.* at 21,027 n.46.

298. *See generally* Edmund L. Andrews & Saul Hansell, *Congress Set to Pass Bill That Restrains Unsolicited E-Mail*, N.Y. TIMES, Nov. 22, 2003, at A1 (noting that “some e-mail experts cautioned that [the Act] includes many concessions to the marketing industry and may have a limited impact”). On the day the House passed the Act, a posting on Nanae, an anti-spam on-line bulletin board, lamented, “Welcome to the death of email, ladies and gentlemen. Would the last person to leave email please turn out the lights?” MCWILLIAMS, *supra* note 61, at 269.

299. *See* Andrews & Hansel, *supra* note 298. Professor David Sorkin said, “[t]he legislation legitimizes spam and will increase the volume.” *Id.*

300. *See* Stephanie Schorow, *Enlarged Spam Law Has Many Frustrated*, BOSTON HERALD, Jan. 7, 2004, at 38.

301. *Id.*

SPAM, to opt-out of receiving messages from each sender.³⁰²

When CAN-SPAM went into effect on January 1, 2004, it had almost no noticeable immediate effect.³⁰³ E-mail users were unpleasantly surprised to find just as many spam messages in their in-boxes on New Year's Day and in the following weeks as they had before the Act took effect.³⁰⁴ It seemed as though the naysayers' predictions had come true: Spammers were ignoring CAN-SPAM.³⁰⁵

One side effect of CAN-SPAM that surprised some was the temporary reduction in commercial e-mail from "legitimate" on-line marketers immediately after the Act went into effect.³⁰⁶ Because CAN-SPAM became law so quickly—only two weeks passed between presidential signature and the law's effective date—many companies did not have time to digest the law and adapt their e-mail strategies to comply with the statute.³⁰⁷ As a result, some companies halted their e-mail marketing efforts until their attorneys analyzed the law and drafted revised policies.³⁰⁸ While CAN-SPAM was not intended to curtail the activities of legitimate marketers, the law reflects good business practices.³⁰⁹ Compliance with the Act does not unduly burden responsible companies, and benefits their customers.³¹⁰

As for the disreputable spammers, they reacted to CAN-SPAM by ignoring it,³¹¹ or by trying to find ways around it.³¹² It has been said that laws are made to be broken, and some spammers saw the passage of CAN-SPAM as a challenge. Spammers looked for loopholes in CAN-SPAM, and some apparently believe they found one in the Act's definition of spam.³¹³ By its express language, CAN-SPAM applies only to messages which have as their "primary purpose ... the commercial advertisement or promotion

302. 149 CONG. REC. S15,947 (daily ed. Nov. 25, 2003) (statement of Sen. Leahy).

303. See Gaither, *supra* note 277. Even one year after enactment, CAN-SPAM's effects had still not been felt. In the year after the law took effect, the volume of spam passing through the Internet increased. See McGuire, *supra* note 5.

304. See Gaither, *supra* note 277.

305. See *id.*

306. See Praed, *supra* note 246.

307. *Marketers Scramble as Spam Law Looms*, CHI. TRIB., Dec. 30, 2003, at C3.

308. See *id.*

309. Praed, *supra* note 246.

310. *Id.*

311. MCWILLIAMS, *supra* note 61, at 295. Studies indicate that not even three percent of post-CAN-SPAM bulk e-mail complies with the Act. *Id.*

312. Jonathan Krim, *Gates Wants to Give E-Mail Users Anti-Spam Weapons*, WASH. POST, Jan. 27, 2004, at E1.

313. *Id.*

of a commercial product or service.”³¹⁴ Shortly after CAN-SPAM took effect, e-mail users began to receive messages purporting to have a “primary purpose” other than advertising.³¹⁵ For example, one message included a list of unusual state laws, like “[i]t is illegal to put tomatoes in clam chowder,” followed by this language: “[t]he primary purpose of this email is to deliver you a ‘Crazy USA State Law of the Week’—The secondary purpose of this email is to let you know: ‘Click Here to Email Advertise Your Web Site to 1,850,000 OPT-IN Email Addresses for FREE!’”³¹⁶ CAN-SPAM does not expressly define “primary purpose,” but it does not seem likely that Congress intended that an e-mail would not be a commercial electronic mail message simply because the sender said that it was not.³¹⁷ While the “primary purpose” loophole does not seem to offer much promise for spammers, creative e-mail marketers will surely seek out and attempt to exploit other potential holes in CAN-SPAM.³¹⁸

Not all spammers flouted or attempted to evade CAN-SPAM.³¹⁹ Alan Ralsky, believed to be one of the most prolific senders of unsolicited commercial e-mail, has decided to comply with the law.³²⁰ Deterred by the penalties that can be imposed by the law, Ralsky modified his practices to include return addresses and the other information required by the law.³²¹

It came as no surprise, however, that most spammers largely ignored CAN-SPAM. Arguably, the primary purpose of enacting the law was not to discourage spammers from sending spam, but rather to establish a uniform system for enforcement.³²² Before CAN-SPAM was enacted, spammers

314. 15 U.S.C.A. § 7702(2)(A) (West Supp. 2004) (emphasis added).

315. See Krim, *supra* note 312.

316. *Id.*

317. See 15 U.S.C.A. § 7701(b)(2) (West Supp. 2004). The Act’s statement of congressional determination of public policy states that “senders of commercial electronic mail should not mislead recipients as to the source or content” of e-mail. *Id.* If there ever was a “primary purpose” loophole, it was closed by a March 2005 revision to the FTC’s CAN-SPAM implementing rules. 16 C.F.R. § 316.3 (2005). Now, the “primary purpose” of an e-mail message is deemed to be commercial if “[a] recipient reasonably interpreting the body of the message would likely conclude that the primary purpose of the message is the commercial advertisement or promotion of a commercial product.” *Id.*

318. Krim, *supra* note 312 (noting that spammers are “trying to exploit loopholes or gray areas in the law”).

319. Saul Hansell, *An Unrepentant Spammer Vows to Carry on, Within the Law*, N.Y. TIMES, Dec. 30, 2003, at C1.

320. *Id.*

321. *Id.* Ralsky said, “[y]ou would have to be stupid to try to violate this law.” *Id.*

322. See 149 CONG. REC. S13,023 (daily ed. Oct. 22, 2003) (statement of Sen. Wyden). Senator Wyden said that it was necessary to create “a uniform, nationwide spam standard” and to develop an “enforcement regime.” *Id.*

claimed that the law was unclear, and some maintained that they were not engaging in illegal activity.³²³ After CAN-SPAM, there is no question that spammers who engage in conduct prohibited by the Act are criminals.³²⁴ It remains to be seen, however, whether the criminal provisions in CAN-SPAM will be an effective deterrent against spammers.³²⁵

Some have predicted that the enactment of CAN-SPAM will result in an exodus of spammers moving offshore to avoid the Act's provisions.³²⁶ This risk may not be as serious as it seems. While offshore relocation may be an attractive option for some spammers who can deliver their products on-line, for example, pornographers and software companies,³²⁷ those spammers who sell physical products, like herbal remedies, however, would likely find it too expensive to operate overseas due to increased shipping costs.³²⁸ Similarly, other spammers who sell services like mortgage refinancing and debt counseling, may find it impractical to relocate offshore.³²⁹ Also, as cooperation among international governments and businesses continues to grow, foreign sites are likely to become increasingly unwelcoming to spammers.³³⁰

B. In Search of the Silver Bullet

Even before it became law, no one expected that the CAN-SPAM Act would be a silver bullet that would single-handedly wipe out the spam problem.³³¹ In fact, the Act's express language admits that it will not solve

323. See Praed, *supra* note 246.

324. See *id.*; see also 149 CONG. REC. S15,944 (daily ed. Nov. 25, 2003) (statement of Sen. Schumer).

325. CAN-SPAM's congressional sponsors urged swift and aggressive enforcement of the Act's criminal provisions. See 149 CONG. REC. S13,023 (daily ed. Oct. 22, 2003) (statement of Sen. Wyden). "[W]e need to see aggressive enforcement action the day this bill is signed into law." *Id.* Six weeks after the Act went into effect, however, not a single arrest had been made. See Cynthia L. Webb, *AWOL on Spam?*, WASHINGTONPOST.COM, Feb. 19, 2004, at <http://www.washingtonpost.com/wp-dyn/articles/A54093-2004Feb19.html>. The first arrests under CAN-SPAM were not made until April 2004. Chris Gaither, *Can Spam Be Canned?*, L.A. TIMES, May 23, 2004, at C3.

326. See Praed, *supra* note 246.

327. See Geoff Hulton, Address at the 2004 Spam Conference at the Massachusetts Institute of Technology (Jan. 16, 2004), available at <http://spamconference.org/webcast.html> (webcast only available on-line).

328. See *id.*

329. See *id.*

330. See Praed, *supra* note 246.

331. See 149 CONG. REC. S15,944 (daily ed. Nov. 25, 2003) (statement of Sen. Wyden). "We are not going to pretend this legislation is a silver bullet because we know that

the spam problem by itself.³³² CAN-SPAM's architects were aware that the Act is only one component of a spam solution that will include regulation, enforcement, consumer education, industry cooperation, and most importantly, technology innovations.³³³

Technological advances can coordinate with CAN-SPAM's provisions to hold spammers accountable.³³⁴ The law establishes a framework of regulation with strong civil and criminal penalties. However, these provisions are useless if law enforcement officials are unable to find spammers and bring them to justice.³³⁵ If computer scientists can develop a means of reliably identifying spammers, law enforcement officials can locate spammers and prosecute them under the law.³³⁶

Technology and law can also attack spam by increasing the costs incurred by spammers. Spam's low cost is one of the characteristics that makes it attractive to marketers.³³⁷ If the cost to send spam exceeds the profits realized by sending the messages, spammers will seek alternate methods of promoting their products and services.³³⁸ If enforced, the civil and criminal fines provided by CAN-SPAM, will significantly raise the cost of spamming, and decrease its attractiveness as a marketing tool. Another way in which spamming costs will increase is if spammers are forced to defend themselves against lawsuits.³³⁹

no piece of legislation is." *Id.*; see also *id.* at S13,021 (daily ed. Oct. 22, 2003) (statement of Sen. McCain). "[T]he odds of us defeating spam by legislation alone are extremely low. The fact that there may be no silver bullet to the problem of spam, however, does not mean that we should stand idly by and do nothing at all about it." *Id.*

332. 15 U.S.C.A. § 7701(a)(12) (West Supp. 2004). The Act's statement of congressional findings and policy notes that "[t]he problems associated with the rapid growth and abuse of unsolicited commercial electronic mail cannot be solved by Federal legislation alone." *Id.*

333. 149 CONG. REC. H12,860 (daily ed. Dec. 8, 2003) (statement of Rep. Sensenbrenner). "Ultimately, spam will be stopped by a combination of new technology, consumer awareness, ISP filtering, and trusted sender systems for legitimate senders of commercial e-mail—with laws and regulation merely setting the outer boundaries of illegitimate e-mail practices." *Id.*; *id.* at S13,024 (daily ed. Oct. 22, 2003) (statement of Sen. Wyden). "We are not going to overpromise. We are not going to say that the day this bill is signed, spam will magically vanish into vapor." *Id.*

334. See Prince, *supra* note 8.

335. 149 CONG. REC. S13,021 (daily ed. Oct. 22, 2003) (statement of Sen. McCain). "[U]nless we can effectively enforce the laws we write, those laws will have little meaning or deterrent effect on any would-be purveyor of spam." *Id.*

336. See Prince *supra* note 8.

337. See *supra* text accompanying notes 59-68.

338. See Praed, *supra* note 246.

339. See *id.* John Praed, an attorney with the Internet Law Group in Washington D.C.,

Some in the software industry are investigating other ways of increasing the cost of spamming by charging spammers to send messages.³⁴⁰ Microsoft has launched the Penny Black Project³⁴¹ to explore ways to reduce the volume of spam by increasing the cost to spammers.³⁴² The project's researchers are testing methods for recipients to charge senders a fee to accept their messages.³⁴³ Under one proposal, an e-mail user could set a high fee for unknown senders and no fee for family members and business associates.³⁴⁴ Another proposal being researched would not use currency, but rather central processing unit (CPU) cycles.³⁴⁵ Requiring that a sending computer "spend" a minimum number of CPU cycles for each message sent limits the total number of messages that can be transmitted from that computer in a day.³⁴⁶ If a spammer wants to exceed that limit, he will have to buy more computers, thereby incurring additional hardware costs, and cutting into his spamming profits by increasing his per-message cost.³⁴⁷ A third proposal under development is "challenge-response" software, which would require senders to verify that

noted that most spammers have limited resources, and they can easily go broke defending themselves against a lawsuit. *Id.* He estimated that two defendants in a suit brought by AOL spent \$20,000 to succeed on a motion to dismiss on the grounds that the Virginia court lacked personal jurisdiction over them. The judge granted the motion, but told the defendants that they could be sued in Florida, and that they should, in fact, be sued. *See id.*

340. Krim, *supra* note 312.

341. *See* MICROSOFT CORP., *The Penny Black Project*, at <http://research.microsoft.com/research/sv/PennyBlack/> (last visited Apr. 14, 2005) [hereinafter *Penny Black Project*]. The first pre-paid, adhesive postage stamp was the Penny Black—so named because it cost one penny, and bore Queen Victoria's likeness printed in black ink. *Id.*; BRITISH BROADCASTING CORP. (BBC), *Timelines*, at http://www.bbc.co.uk/history/timelines/britain/vic_penny_black.shtml (last visited Apr. 14, 2005). The Penny Black revolutionized the British postal system when it was introduced in the 1830s. *See Penny Black Project, supra*. Prior to the Penny Black, costs for mailing letters and packages were typically borne by the recipient, but the Penny Black shifted the cost of mailing to the sender. The analogy to the spam problem is clear: Currently, the recipient bears most of the costs associated with spam. *Id.*; *see also supra* text accompanying note 63. If those costs could be shifted back to the sender, it would become less profitable, and therefore less desirable for spammers to send unsolicited messages. *Penny Black Project, supra*.

342. *Penny Black Project, supra* note 341.

343. Krim, *supra* note 312.

344. *See id.*

345. *Penny Black Project, supra* note 341.

346. *See id.* "[T]here are about 80,000 seconds in a day," so imposing a computational "price" of ten seconds per message would mean that a spamming computer could send no more than 8000 messages each day. *Id.*

347. *See id.*

2005]

CAN-SPAM ACT OF 2003

1003

messages are sent by an actual human being, and not by a bulk mailing program.³⁴⁸ Any message that is not verified would be rejected by the recipient. The requirement of human intervention in the spamming process will dramatically increase the staffing costs borne by spammers. These technology-based payment schemes are still in development, and some e-mail experts are skeptical about their effectiveness, and their potentially stymieing effect on e-commerce.³⁴⁹

CONCLUSION

In a very short time, spam has grown from a simple annoyance to a serious problem demanding Congress's attention. By passing CAN-SPAM, Congress has taken a step toward alleviating the enormous pressure spam has placed on the economy, the patience of e-mail users, and the infrastructure of the Internet. The Act's congressional sponsors believe that the statute will reduce the worst kinds of spam. CAN-SPAM's critics are doubtful that it will have any effect, except to perhaps increase the amount of spam e-mail users receive. The Act's effect on the spam problem remains to be seen, and all of the players in the spam war are waiting and watching.

In the end, legislation like CAN-SPAM is going to play only a small role in solving the spam problem.³⁵⁰ The real solution is going to come in the form of technological developments and industry best practices. CAN-SPAM's role in addressing the spam problem is to provide law enforcement officials with tough criminal provisions to prosecute the worst spammers, and to set boundaries for commercial e-mail that are flexible enough to allow for continued development in technology and e-commerce.³⁵¹

Adam Hamel

348. Krim, *supra* note 312.

349. *See id.*

350. 149 CONG. REC. H12,198 (daily ed. Nov. 21, 2003) (statement of Rep. Stearns). "Legislation is only part of the solution, and in my view a smaller part." *Id.*

351. *See id.* at H12,194 (daily ed. Nov. 21, 2003) (statement of Rep. Goodlatte). "Because no legislation can provide a cure-all for spam, this bill is technology-friendly. It protects the ability of ISPs and small businesses to develop innovative technological solutions to combat spam and to protect consumers, such as filtering and blocking technologies." *Id.*; *see also id.* at S13,019 (daily ed. Oct. 22, 2003) (statement of Sen. McCain).

1004

NEW ENGLAND LAW REVIEW

[Vol. 39:961
